

Gen. LUIGI SACCO



UN PRIMATO ITALIANO

LA CRITTOGRAFIA NEI SECOLI XV E XVI



ISTITUTO STORICO E DI CULTURA DELL'ARMA DEL GENIO
ROMA 1958

*Estratto dal Bollettino dell'Istituto Storico e di
Cultura dell'Arma del Genio - fasc. 26, dicembre 1947.*

Stampato nel maggio 1958 dal
21° Stabilimento Trasmissioni
Roma

Gen. LUIGI SACCO

1 2 3 4 5

UN PRIMATO ITALIANO

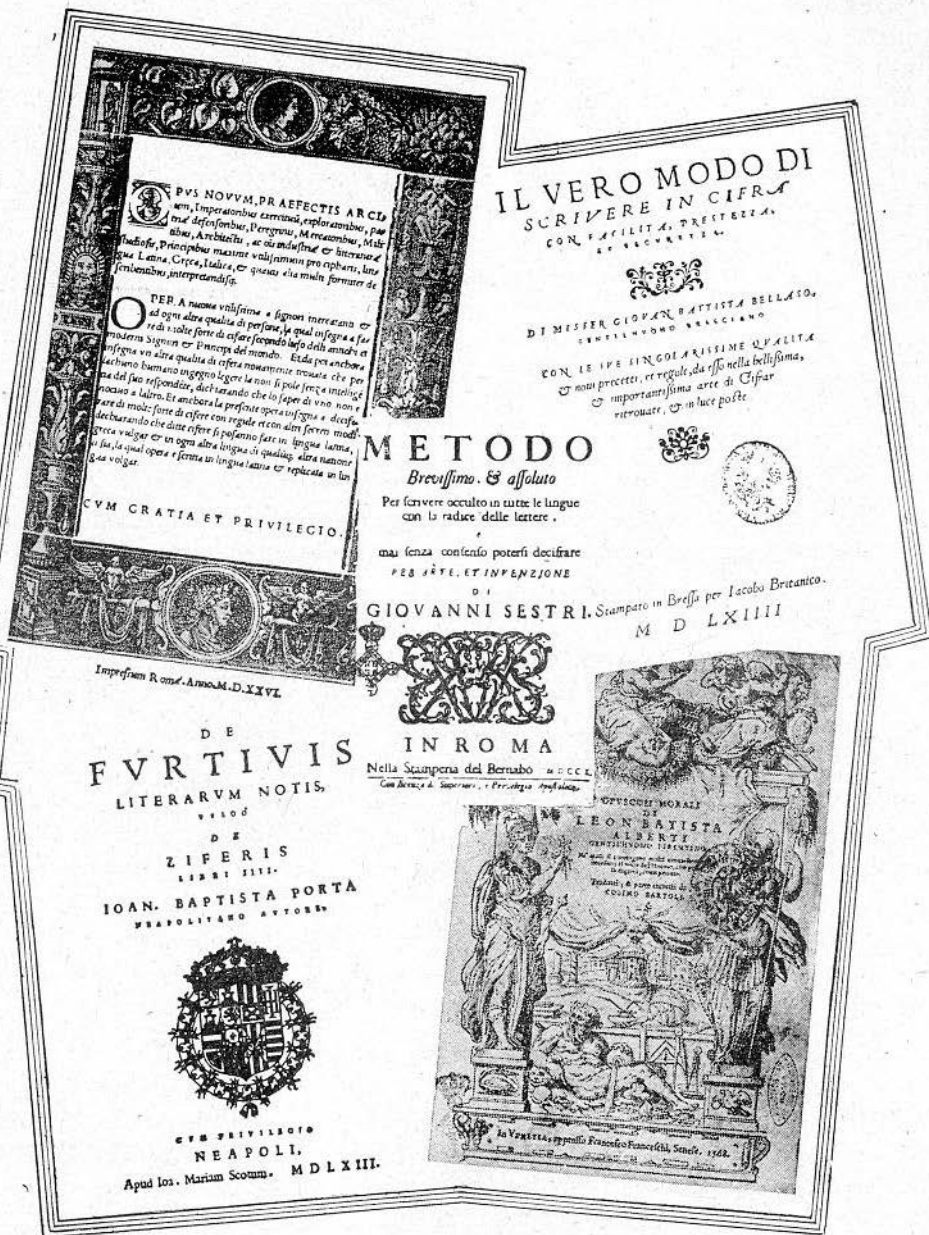
LA CRITTOGRAFIA NEI SECOLI XV E XVI



ISTITUTO STORICO E DI CULTURA DELL'ARMA DEL GENIO
ROMA 1958

FRONTESPIZI

di opere italiane di crittografia dei secoli XV, XVI e XVII



- | | |
|-------------------------------|--|
| In alto a sinistra | Iacopo SILVESTRI - Roma 1526 |
| In alto a destra | G. B. BELLASO - Brescia 1564 |
| Al centro | Giovanni SESTRI - Roma 1710 |
| In basso a sinistra | Giov. Batt. PORTA - Napoli 1563 |
| In basso a destra | Leon Batt. ALBERTI (traduzione Bartoli) - Venezia 1568 |

UN PRIMATO ITALIANO

LA CRITTOGRAFIA NEI SECOLI XV e XVI

di LUIGI SACCO

1. *Origine e scopi della crittografia.*

Dopo secoli di vita nascosta e pressoché ignorata, la *crittografia*, l'arte cioè di scrivere segretamente, usciva dai ben celati uffici cifra dei diplomatici per diffondersi in molti e nuovi ambienti, specie militari, allorquando, circa un secolo fa, il telegrafo aveva reso possibili comunicazioni comode e rapide ma facilmente intercettabili da estranei e da nemici: questo grave difetto, molto aggravatosi con lo avvento della Radio, non poteva rimediarsi se non cifrando le comunicazioni esposte alle indiscrezioni dei curiosi interessati.

Per adattarsi alle nuove esigenze i *cifristi* dovettero bensì modificare un poco la forma dei loro crittogrammi, ma non rilevarono subito che l'aumentata possibilità di intercettazione avrebbe acuito il desiderio di conoscere le notizie celate nei sempre più numerosi dispacci cifrati che si potevano raccogliere: non si avvertì cioè che la telegrafia avrebbe inevitabilmente stimolato il progredire della *decrittografia*, l'arte che si propone di interpretare le cifre, svelandone il segreto, senza possedere le chiavi della cifratura. Questo è infatti quello che avvenne e di ciò abbiamo un chiaro indizio nella rifiorente letteratura crittografica dovuta specialmente alla scuola francese, che verso la fine del sec. XIX diede un decisivo impulso a questo genere di studi. Una concomitante evoluzione avvenne naturalmente anche nella crittografia pratica, in quella cioè degli uffici cifra, ma essa si manifestò con un sensibile ritardo e solo dopo che evidenti e gravi danni erano derivati da questo sfasamento tra la crittografia offensiva (*decrittografia*) e quella, difensiva, delle cifre in uso. In realtà la storia della crittografia, specie di quella moderna, mostra una singolare tendenza dei cifristi a preferire i vecchi procedimenti, più comodi,

contro quelli nuovi, anche se più segreti; la cosa è d'altronde spiegabile, ma ha spesso dato luogo a gravi inconvenienti, dovuti alla fallace illusione di possedere, nella cifra, un linguaggio segreto di cui si può usare senza eccessive precauzioni, il che non sempre risponde a verità.

Un solo rimedio sembra efficace contro il possibile ripetersi di una tale illusione, ed è la diffusione della cultura crittografica, cioè la conoscenza approfondita delle possibilità decrittografiche, da parte non solo di chi deve cifrare, ma altresì dei capi che affidano ai cifristi le comunicazioni che dovrebbero rimanere segrete. Ciò spiega l'interesse crescente attribuito alla crittografia in questi ultimi anni; interesse molto spinto in Francia ed in America, ove si notano altresì le più frequenti pubblicazioni su quell'arte.

Un esagerato timore di tutelare segreti di Stato potrebbe indurre a parlare ed a scrivere il meno possibile di crittografia, ma l'ignoranza che in tal modo si manterrebbe sui procedimenti crittografici, tornerebbe tutta a danno di chi desidera e coltiva tale ignoranza, perché essa creerebbe un ambiente incapace di apprezzare il vero valore delle cifre usate, ed altresì molto adatto per commettere le più deplorabili ingenuità nell'uso delle cifre, ingenuità che non mancherebbero di essere sfruttate dai più colti e smaliziati nemici.

E' norma elementare che per ben difendersi è necessario conoscere i mezzi di offesa, nè può farvi eccezione la lotta crittografica; e nulla lascia credere che essa non sarà più combattuta in avvenire.

Queste considerazioni ci hanno indotto a scrivere di crittografia anche su questo Bollettino (1) che, dedicato all'Arma del Genio ed alle Trasmissioni, è direttamente interessato alla guerra delle cifre e quindi anche alla loro storia; e poichè questa costituisce un indiscutibile vanto italiano, vogliamo sperare che la sua conoscenza tornerà gradita agli italiani e servirà loro di incitamento a coltivare un'arte che non esige materie prime nè risorse finanziarie a noi inaccessibili.

Non intendiamo, con le sommarie notizie che seguono, di presentare una storia della crittografia, e neppure della sola crittografia

(1) Per maggiori notizie su quest'arte si rimanda al recente *Manuale di crittografia* di LUIGI SACCO - 1947, Roma - (374 pagg., 24 figg., 28 tav.).

italiana, ma solo ci proponiamo un rapido esame della letteratura crittografica, a cominciare dalle più antiche opere note, nonché delle cifre contemporaneamente in uso, per dimostrare il posto preminente che spetta agli Italiani nella creazione e nello sviluppo iniziale sia della crittografia che della decrittografia. Tale primato a dir vero ci è generalmente riconosciuto, ma non sempre con convinzione e non sempre nella sua pienezza, quale risulta dall'esame un poco approfondito, che ora inizieremo, dei documenti, alcuni dei quali peraltro rimasti ignoti o poco noti anche agli scrittori di crittologia più coscienziosi.

2. Nasce in Italia la crittografia moderna.

Cominciamo con l'osservare che il livello crittografico in Italia alla fine del medioevo era notevolmente più elevato che negli altri paesi. Il Meister (2), che ha compiuto le più accurate indagini negli archivi tedeschi, spagnoli ed italiani, rileva che mentre ancora nel 1460 in Germania si usava cifrare le sole vocali, e talvolta anche le consonanti ma con semplici sostituzioni letterali, in Italia erano usati, fin dall'inizio del 1400, alfabeti e nomenclatori molto complessi che ancora esistono negli archivi di Venezia, Milano, Mantova, Genova, Modena, Ferrara, Firenze, Lucca, Siena, Pisa, Urbino, Roma.

La crittografia appare, così, strettamente collegata alla diplomazia, che pure nacque in Italia con la istituzione delle prime ambasciate permanenti, iniziate, secondo il Meister, dagli Sforza di Milano a metà del XV secolo; ma già gli ambasciatori occasionali precedenti erano normalmente muniti di cifre, di una certa complicazione, sin dalla fine del XIV secolo. La fig. 1 mostra una cifra veneziana del 1411, ancora relativamente semplice, ma già ad Urbino, nel 1440, ne troviamo una (fig. 2) che ha molti segni *omofoni* (cioè che cifrano una stessa lettera), molti segni nulli, nonché un nomenclatore, di 114 voci, che non segue l'ordine alfabetico né nel chiaro, né nel cifrato, indizi questi di una notevole maturità crittografica. La fig. 2 è tratta dal Codice Urbinato che si conserva in Vaticano e che contiene 72

(2) A. MEISTER, *Die Anfänge der Modernen Diplomatischen Geheimschrift* - Paderborn, 1902.

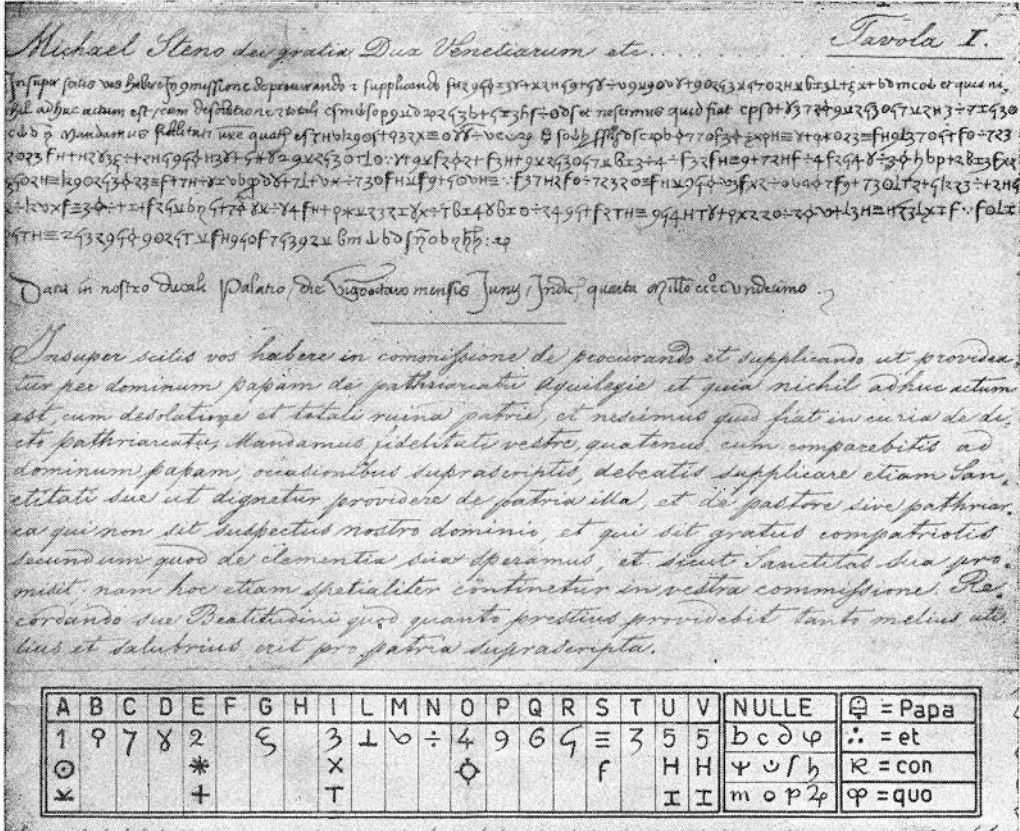


Fig. 1 — Esempio di cifra completa veneziana (1411)

cifre, analoghe a quella qui esposta, con le quali Federico da Montefeltro, poi Duca d'Urbino, corrispondeva con i suoi confidenti e con molti principi italiani. Queste cifre, finora ignorate dai crittologi, sono analoghe ma più complete di quelle usate dagli altri principi italiani in quell'epoca (metà del 1400) ed in netto anticipo sulle contemporanee tedesche (3).

(3) A. MEISTER (*loc. cit.*, pag. 12).

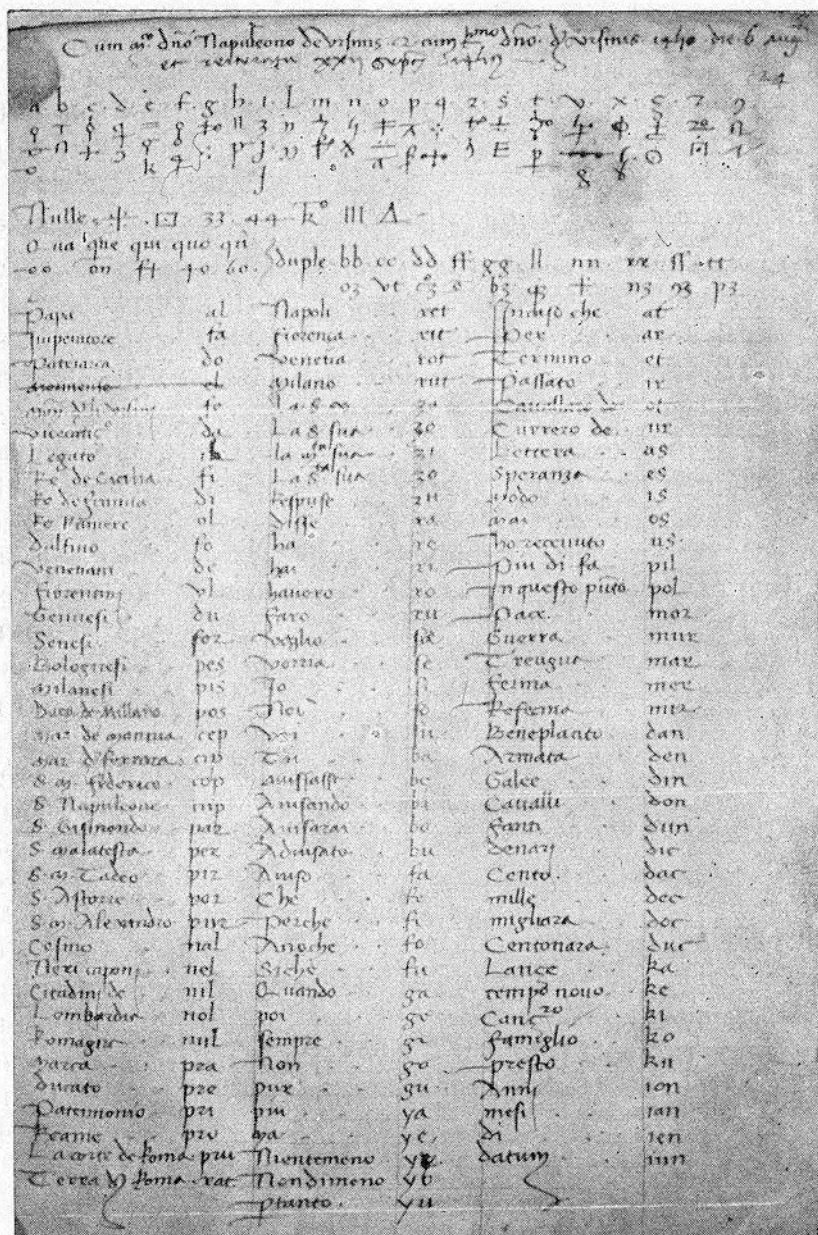


Fig. 2 — Riproduzione di una pagina del Codice urbinatense (1440).

Dello stesso valore erano quelle usate in Francia da Enrico IV (4) al principio del 1600 ed in Ispagna nella stessa epoca (5).

Nessuna meraviglia quindi che da un tale ambiente siano sorte le prime ricerche teoriche e pratiche sui procedimenti crittografici.

3. *Il Trattato di Leon Battista Alberti.*

E' da tutti riconosciuto che il più antico trattato di cifre (se si esclude un capitolo dedicato a queste nel « Trattato delle fortezze » di Enea il Tattico, 390 av. Cristo), è quello di Leon Battista ALBERTI (1404-1472) che si conserva manoscritto negli Archivi Vaticani ed in quelli Chigiani e Veneti; una traduzione italiana trovasi nelle « Opere morali » di L. Battista Alberti — tradotte da C. Bartoli, Venezia, 1568 (fig. 3) — rimasta però finora pressoché ignorata dai crittologi.

Scritto verso il 1466÷70 esso è non solo il trattato più antico ma, come ora vedremo, altresì il più geniale e lungimirante tra quanti ne siano comparsi dopo di lui nei successivi quattrocento anni. Per onorare la memoria di questo insigne umanista ed altresì per documentare quanto scriviamo di lui, diamo in appendice la traduzione del suo Trattato, compiuta con rara competenza dal Reverendo Mons. Filippo Cenci (6) che qui sentitamente ringraziamo.

L'Alberti si accinse a scrivere il suo Trattato per invito di Leonardo Dato, segretario pontificio sotto Paolo II (1464-1471), e comincia con l'osservare che può essere utile interpretare le cifre altrui, ma più utile è garantire il segreto delle proprie. Per giungere a tanto egli premette una analisi diligente della scrittura ordinaria, rilevando subito che le parole sono composte di sillabe e di lettere, che a loro volta si dividono in consonanti e vocali. Considerate varie forme letterarie (latine), egli trova in tutte una lieve preponderanza statistica di consonanti, press'a poco nella proporzione di 400 consonanti contro 300 vocali: la E e la I sono le vocali più frequenti, seguono A, O, U.

(4) P. VALERIO, *De la cryptographie* (2.e partie) - Paris, 1896 (pag. 95).

(5) G. CARMONA, *Tratado de criptografia*, 1894, Madrid (pag. 181-192).

(6) Si sono omesse le note del traduttore, che rivelano varii errori di trascrizione e di stampa del testo latino, limitandoci ad annotare alcuni punti meno sicuri. Il testo latino è riportato nel « A. MEISTER, *Die Geheimschrift im Dienste der Päpstlichen Kurie* » - Paderborn, 1906 - pag. 125-141.

Esamina quindi i dittonghi più frequenti e quelli più rari e passa alle consonanti, per distinguere ancora le più frequenti dalle più rare, per ricavare le più comuni sequenze di sole consonanti, sia in latino che in volgare.

Da questa sua accurata analisi egli deduce, e fissa in poche parole, il procedimento più razionale da seguire per la soluzione delle cifre allora usate. In queste cifre varie lettere erano sostituite con i segni grafici più disparati, con largo uso di segni nulli, di segni *omofoni* (cioè significanti tutti una stessa lettera chiara), ed erano scritti senza



Fig. 3 — Riproduzione del frontespizio dell'opera di L. B. Alberti tradotta dal Bartoli

separare le parole cifrate. Ora è importante notare che i decrittatori successivi, se si eccettua Giov. Batt. Porta di cui diremo in seguito, fino a giungere ai più diligenti tedeschi del sec. XVIII, non affrontano mai queste cifre complesse, limitandosi a quelle, moltissimo più semplici, in cui ogni lettera è sostituita da un solo segno, quindi senza omofoni e senza nulle, e che conservano la separazione delle parole (7). Bisogna giungere al Valerio (8) per ritrovare, sia pure ampliata, una analisi completa e generale come quella dell'Alberti.

Passando quindi a ragionare delle cifre da adottare, oltre a precisare le regole per la scelta dei segni omofoni, cosa tuttavia già praticata a quell'epoca (fig. 1 e 2), egli insiste sulla preparazione dei testi chiari prima di cifrarli, consigliando di abbreviarli, di scrivere senza osservare l'ortografia e frammezzando delle nulle; in modo cioè da sfuggire il più possibile alle regole trovate per la decrittazione. Consiglia quindi l'aggiunta di un nomenclatore, nel quale intere sillabe, o parole, o frasi, sono rappresentate da un solo segno o dalla combinazione di più segni, come d'altronde pure già usavasi, ed accenna quindi alle cifre per trasposizione, cioè ottenute alterando l'ordine delle lettere chiare secondo regole convenute, notando però che esse non sono sicure.

Parla poi del linguaggio convenzionale, nonché di quello dissimulabile in messaggi chiari apparentemente innocui; ricorda, derivandoli, gli inchiostri cosiddetti simpatici ed accenna a vari modi per celare materialmente i messaggi segreti, per giungere infine al suo disco cifrante, che mostra tutta la genialità del suo inventore.

4. Il disco cifrante di L. B. Alberti.

Il disco cifrante dell'Alberti (fig. 4) comprende due cerchi concentrici di cui uno per il testo chiaro e uno per il cifrato. Mentre questo porta 24 delle 26 lettere latine (escluse V, W, J ed incluso &), l'altro ne porta solo 20, i rimanenti quattro posti essendo riempiti con i numeri 1, 2, 3, 4: si dovrà quindi rinunciare, nel testo chiaro, ad usare le lettere V, W, H, J, K, Y. Nel disco chiaro le lettere sono

(7) LUIGI SACCO (op. cit. n. 149).

(8) P. VALERIO, *De la cryptographie* (1.e partie), 1893, Paris.

maiuscole e disposte in ordine alfabetico; nel cifrato sono minuscole e *disordinate*. In ogni posizione del disco, ad una lettera chiara (*decifra*) corrisponde una *cifra*: si possono così ottenere 24 alfabeti diversi mettendo ogni volta una diversa lettera (*chiave*) del disco chiaro di fronte ad una lettera fissa del cifrato (*indice*), ad es. x.

L'Alberti mostra così come si possa cambiare di alfabeto a piacimento con la sola cura di indicare al corrispondente, nel crittogramma, la lettera chiave del nuovo alfabeto, che, per essere maiuscola mentre il testo cifrato è minuscolo, indicherà senza equivoci il cambio dell'alfabeto. E' questo il primo esempio di *cifra polialfabetica a chiave e con alfabeti disordinati*, che viene inoltre complicata dall'Alberti con il geniale uso di *lettere nulle*.

Egli consiglia a questo scopo di intercalare, a caso nel testo da cifrare, uno dei numeri: 1, 2, 3 o 4 e di mettere al loro posto, nel crittogramma, le lettere minuscole che ad esse corrispondono, nell'alfabeto in vigore in quel punto, lettere da ritenere nulle.

Subito dopo l'Alberti, considerato il pericolo che le maiuscole indicanti la chiave, frammezzate a quelle minuscole del crittogramma, tradiscano il cambio dell'alfabeto, vi rimedia suggerendo di prendere l'*indice* nel chiaro, ad es. B, e la *chiave* nel cifrato, cominciando

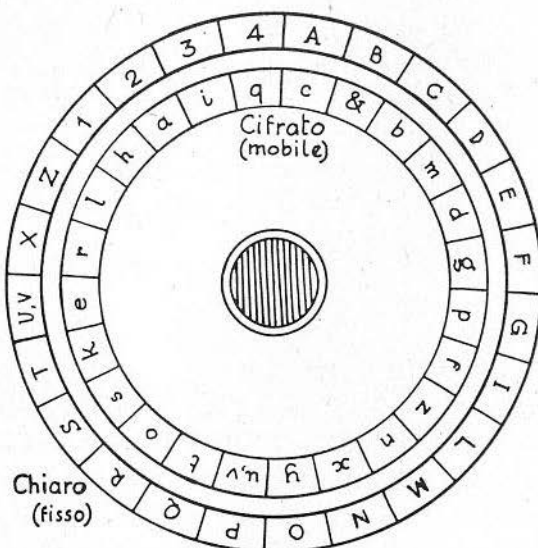


Fig. 4 — Disco cifrante da L. B. Alberti

il crittogramma con la chiave convenuta, ad es. q, che, posta nel disco sotto l'indice B, individua l'alfabeto iniziale. Quando poi si vuol cambiare l'alfabeto, basterà inserire nel testo chiaro uno dei quattro numeri 1, 2, 3, 4, e, nel cifrato, la lettera minuscola ad esso affacciata nel disco: questa minuscola non avrà più il significato di nulla come prima, ma sarà la nuova chiave che il decifrista riconoscerà perché essa corrisponde ad un numero isolato; dopo di ciò egli roterà il disco interno in modo da portare quella lettera sotto l'indice B e così avrà determinato il nuovo alfabeto, senza equivoci. In tal modo nessun segno esteriore nel crittogramma tradirà il cambio della chiave, che diventa perciò un nuovo decisivo elemento di segreto. La cifra così ottenuta presenta le seguenti brillanti caratteristiche: è composta di sole lettere minuscole; usa 24 alfabeti disordinati: questi sono cambiabili ad arbitrio del cifrista; il cambio risulta celato al decrittatore. Cifra quindi quanto mai moderna e sicura: affidata a un cifrista un poco addestrato, essa darebbe ancor oggi del filo da torcere ai più provetti decrittatori, anche senza la ulteriore complicazione suggerita dall'Alberti, consistente nell'introdurre saltuariamente, nel crittogramma, delle lettere maiuscole da considerare come nulle.

Chiude il trattato un terzo modo, non meno geniale dei precedenti, di servirsi dei quattro numeri del disco chiaro; modo che anticipa di quattro secoli un artificio tuttora in uso e cioè la *sopraccifatura* dei repertori disordinati.

Egli propone infatti di compilare una lista di 336 gruppi cifranti, ottenuti raggruppando in tutti i modi i quattro numeri suddetti, e cioè: 16 gruppi (4^2) di due numeri 11, 12, 13, 14, 21, 22, 23, ... 44); 64 gruppi (4^3) di tre numeri da 111 a 444) e 256 gruppi (4^4) di quattro numeri da 1111 a 4444); in tutto 336.

Contemporaneamente egli consiglia un'altra lista di 336 nomi propri, voci grammaticali ed intere frasi, disposte secondo l'ordine alfabetico delle loro lettere iniziali, in modo da renderne facile la ricerca: però, e qui sta il primo geniale artificio, non si debbono far corrispondere le voci chiare ordinate ai gruppi numerici pure ordinati, ma bensì, ai gruppi numerici ordinati della prima lista, si faranno corrispondere voci chiare disordinate; quindi, raggruppate e riordinate queste nella seconda lista, vi si faranno corrispondere i gruppi numerici ricavati dalla prima lista, in modo che la 1^a lista serva per cifrare

e l'altra per decifrare; queste operazioni risultano quindi ugualmente comode mentre resta esclusa ogni corrispondenza regolare tra voci e gruppi, corrispondenza che sarebbe esiziale pel segreto.

L'Alberti ha dunque visto chiaramente la debolezza dei codici detti *cifranti-decifranti*, escogitati circa 100 anni fa e che erano ancora in uso generale al principio del XX secolo: in essi, in un'unica lista, alle voci chiare ordinate, corrispondono gruppi numerici pure ordinati, in modo da rendere comoda la ricerca sia cifrando che decifrandolo, ma con enorme riduzione del segreto.

Egli scarta decisamente questo modo e consiglia le due liste distinte, che troviamo poi, due secoli dopo, in Francia ai tempi del Re Sole (9). Ma non si arresta a questo punto la genialità dell'Alberti, perché egli non propone già di sostituire, nel crittogramma, i gruppi numerici ricavati dalla seconda lista, ma bensì di mettere al loro posto le lettere minuscole che vi corrispondono sul disco cifrante, nella posizione in vigore in quel punto. Così le voci chiare risultano due volte cifrate: la prima coi numeri ricavati dalla seconda lista, poi con le lettere ricavate dal disco; esse sono cioè, come ora si dice, *sopracifrate* e con 24 alfabeti disordinati ed usati promiscuamente con chiavi nascoste ai decrittatori. Non si deve infatti dimenticare che l'uso dei gruppi di 2, 3, 4 numeri come cifranti delle voci del repertorio, non esclude l'uso dei quattro numeri *isolati* come indicatori del cambio dell'alfabeto; i due modi si completano, anzi mirabilmente. E' poi importante rilevare che mentre le liste separate per cifrare e per decifrare si sono introdotte solo nel XVII secolo, la sopraccifatura dei relativi gruppi si ebbe solo al principio del XX secolo.

Il solo difetto che sembra attribuibile al disco dell'Alberti è la sua forma, che ne rende scomodo l'uso, mentre questo sarebbe stato più agevole se gli alfabeti si fossero ricavati su regoletti scorrevoli. Inoltre, l'aver egli consigliato di mantenere il segreto su di esso ne ha impedita la diffusione, che in realtà non si ebbe neppure dopo che, nel 1568, il Bartoli pubblicò la traduzione del « *Trattato della cifra* » rimasta quasi nascosta in mezzo ad altre opere morali dello stesso Alberti: questi era d'altra parte troppo in anticipo sui suoi tempi.

(9) L. Sacco - loc. cit. n. 134.

Il solo autore che cita l'Alberti come crittologo è il francese B. de Vigenère (10) che mostra di aver bensì conosciuto la traduzione del Bartoli ma non di averne capita l'importanza (11). L'Alberti, con la sua limpida ed acuta logica, costituiva una vetta dalla quale non si poteva che discendere, il che avvenne infatti, e gradualmente, fino a ridurre, durante il XIX secolo, quasi infantili le cifre, comprese quelle diplomatiche e militari.

5. *Le regole decrittografiche di Cicco Simonetta.*

Dopo esserci trattenuti alquanto sull'Alberti, che bene se lo merita, ci sarà ora facile mostrare come i successori si siano preoccupati eccessivamente di ingraziarsi i cifristi, che sovente aborriscono dalle complicazioni anche solo apparenti. Essi hanno infatti cercato cifre sempre più semplici, di certo ritenendole sufficientemente segrete per il fatto che mancò loro la percezione delle debolezze che essi introducevano con le semplificazioni, debolezze che erano state chiaramente viste dall'Alberti.

Prima però dobbiamo accennare ad un altro pioniere nel campo della decrittografia.

Immediatamente dopo l'Alberti troviamo infatti nel 1474, un opuscolo di Cicco SIMONETTA, importante personaggio della corte degli Sforza a Milano, ma di origine napoletana e finito tragicamente sul patibolo nel 1480, per ordine di Ludovico il Moro. Come mostra la traduzione che riportiamo in appendice N° 2 (dovuta alla cortesia del colonnello A. Casola), le tredici regole del Simonetta sono applicabili solo alle cifre senza omofoni, senza nulle ed a parole staccate, cifre che si potevano ritenere già sorpassate nel 1474 in Italia: egli stesso **constata**, alla fine, che sarebbe facile rendere inoperanti le sue regole di decrittazione, mediante semplici complicazioni nel cifrare. Le regole del Simonetta, molto pratiche e chiare, completano, in certo modo, quelle più generali ed astratte dell'Alberti.

(10) BLAISE DE VIGENERE, *Traicté des chiffres* - 1587, Paris - pag. 209.

(11) L. SACCO - loc. cit. n. 144, pag. 298.

6. Il contributo di Jacopo Silvestri.

Dobbiamo ora tornare a Roma, dove nel 1526 venne stampato il primo trattato italiano di cifre (12) dovuto a Jacopo SILVESTRI, fiorentino, che sembra abbia conosciuto il manoscritto dell'Alberti, perché ne imita l'introduzione. Anche Silvestri descrive un disco cifrante ma con i due alfabeti, chiaro e cifrato, entrambi regolari e di egual numero di lettere; non si scorge nel Silvestri l'idea dello alfabeto da cambiare nel corso del crittogramma, segnalando la chiave al corrispondente: al più si può interpretare la sua poco chiara esposizione pensando che egli intendesse di cifrare le successive lettere del chiaro in consecutive posizioni del disco mobile, spostato ogni volta di un posto. Anche Silvestri in seguito propone l'uso di molti alfabeti, ma senza dare regole né esempi: siamo molto al disotto dell'Alberti.

Analogo abbassamento si nota nel nomenclatore proposto dal Silvestri, che, anziché di due distinte liste per cifrare e decifrare, comprende una sola lista di voci chiare ed ordinate, cui corrispondono cifre (costituite da gruppi di lettere e numeri) comprendenti due parti, una comune a tutte le voci aventi la stessa iniziale ed elencate nella stessa lista, l'altra indicante il numero della riga in cui la voce si trova elencata nella lista. E' esattamente il principio del *cifrario paginato*, poi adottato nei primi codici telegrafici segreti, apparsi verso il 1850, ma che rappresentano un grave peggioramento rispetto al cifrario a voci disordinate dell'Alberti. Anche il Silvestri tratta del decrittamento, seguendo Alberti e Simonetta, però con uno stile alquanto prolisso ed oscuro.

7. Le chiavi e l'opera di G. B. Bellaso.

La citata opera del Silvestri, che ebbe una discreta diffusione e notorietà, mostra in ogni caso che a Roma, nella prima metà del 1500, accanto alle arti belle di Raffaello e di Michelangelo, fervevano anche gli studi sulla crittografia. Questo ci è confermato dall'autore francese già citato, B. Vigenère, che trovandosi a Roma come addetto all'ambasciata di Francia fin dal 1549, dice che vi si trovavan abili

(12) J. SILVESTRI, *Opus novum praelectis arcium, etc. etc.* - Roma, 1526 (v. frontespizi).

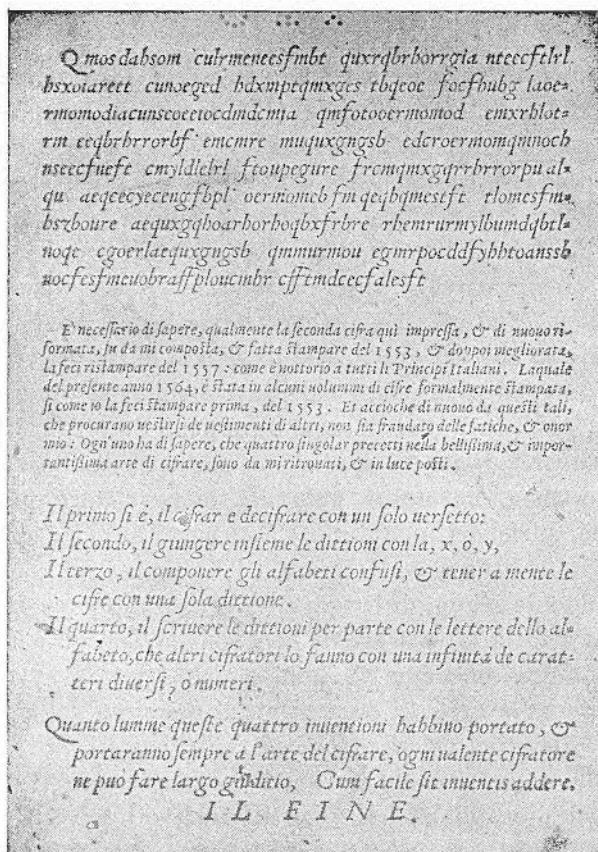


Fig. 5 — Riproduzione dell'ultima pagina dell'«opuscolo» di Bellaso.

decrittatori e cita il priore di S. Pietro, che in poche ore aveva decrit-
 tate intere pagine cifrate in turco, «di cui non conosceva quattro
 parole». In quel periodo il Vigenère conobbe un bravo crittologo in
 G. B. BELLASO, bresciano, cui attribuisce l'invenzione della cifra
 a chiave, mostrando così di non aver conosciuta o di non aver capita
 l'opera dell'Alberti. Il Bellaso infatti nel 1553 aveva fatto stampare
 un suo opuscolo (13) che ebbe altre due edizioni nel 1557 e nel 1564,

(13) G. B. BELLASO - *Il vero modo di scrivere in cifra* - Brescia, 1564 (v. fron-
 tespizi).

nel quale espone delle geniali idee per la formazione di un alfabeto disordinato, derivandolo da una sola parola convenuta, versetto o motto; in esso egli dà inoltre varie regole per l'uso di diversi alfabeti derivati dal primo (tutti disordinati), mediante altre parole *chiavi*, che individuano gli alfabeti da usare. Egli fornisce poi il primo esempio di *autociframento*, cioè di una cifra in cui il cambio dell'alfabeto è comandato dallo stesso testo chiaro che si trasmette, e chiude con un originale repertorio a gruppi cifranti, variabili secondo una chiave convenuta.

Il Bellaso, che è stato preceduto dall'Alberti nella cifratura con diversi alfabeti disordinati, segna un progresso sull'Alberti prescrivendo che l'alfabeto indicato dalla lettera chiave sia usato solo per la lettera chiara immediatamente seguente, mentre le lettere successive vanno cifrate con i successivi alfabeti derivati da quello scelto. Per contro l'Alberti, mentre lasciava la facoltà di usare lo stesso alfabeto per varie lettere consecutive, celava meglio il cambio della chiave. Gli alfabeti del Bellaso, pur essendo disordinati sono però meno segreti di quelli dell'Alberti perché *involutori* o reciproci, cioè costituiti da dodici coppie di lettere, ciascuna lettera di una coppia essendo cifrata e decifrata con l'altra della stessa coppia, il che, se semplifica la tabella cifrante, agevola pure la decrittazione.

Comunque il Bellaso è da considerare come un geniale innovatore che è stato però poco fortunato, specie per la scarsa diffusione del suo opuscolo; questo d'altronde aveva scopi relativamente limitati, specialmente nei confronti del contemporaneo volume di Giovanni Battista Porta, opera di ben più ampio respiro e che ha assorbito, modificandole, le idee del Bellaso.

8. *I primi Uffici Cifra (Roma, Venezia, Firenze, ecc.).*

Prima di trattare dell'opera di Gio. B. Porta che per vastità, varietà e serietà di argomenti, nonché per la sua notorietà fu sempre considerata come un testo classico della crittografia, conviene riportarci per un momento all'ambiente dei cifristi italiani addetti alle varie cancellerie, per constatare in molti di essi un vivo fervore di studi e di ricerche ed una non comune abilità.

A Roma si costituisce una segreteria delle cifre verso il 1540 con Antonio ELIO, poi vescovo di Pola, al quale si deve probabilmente

una cifra molto originale, che per oltre 50 anni fu largamente usata dalla diplomazia pontificia e che trova un riscontro solo nell'opera del Cardano di cui diremo in seguito.

Si tratta della *cifra a polifoni*, mediante la quale si riesce a cifrare le 20 lettere più usate, ciascuna con uno solo dei dieci numeri, ottenendo inoltre dei crittogrammi costituiti di soli numeri e non meno ermetici degli altri (14).

A Venezia dal 1506 un valente cifrista, Giovanni SORO, acquistava grande fama di decrittatore e nel 1539 compilava un suo « liber zifrarum », con le regole per risolvere le cifre italiane, latine, spagnole e francesi, disgraziatamente andato perduto.

La sua fama era tanto diffusa che il 27 aprile 1530, venuto in visita ufficiale a Venezia il principe di Salerno, questi chiese come un favore speciale, di conoscere Pietro Bembo, Marin Sanudo e Giovanni Soro da lui chiamato « Zuan dalle cifre ». Soro aveva già infatti risolte ripetutamente per conto del Papa delle cifre intercettate a partire dal 1510. Nel 1526 egli aveva ancora decrittati tre lunghi dispacci scambiati tra Carlo V ed i suoi fautori a Roma ed intercettati dalla corte papale. Dal diario di Marin Sanudo risulta che il Soro era in Francia tenuto per un Dio perchè aveva decrittate lettere mandategli in esame da Poitiers. Nell'agosto del 1529 il Papa Clemente VII, per provare una cifra usata con il suo legato in Francia, la sottopose al Soro che non essendo riuscito a decrittarela tranquillizzò il Papa sulla sua ermeticità.

L'impulso dato dal Soro alle cifre veneziane diede altri frutti nei « Trattati di cifre » di Francesco MARIN (1578) e di Agostino AMADI (1588) dei quali parlano ampiamente Pasini (15) e Meister (16). Sono « Trattati » più o meno ampi, specie di istruzioni pratiche, segrete, destinate ai cifristi e che confermano la importanza che i veneziani attribuivano alla cifra, imitati in ciò dalle principali altre Signorie italiane. Così a Firenze un abile e molto segreto ufficio cifra era affidato al conte Pirro MUSEFILI della Sasseta, del quale si conservano molti dispacci cifrati stranieri da lui decrittati tra il 1546 e il 1557.

(14) L. SACCO - Loc. cit., N. 20, pag. 23.

(15) L. PASINI, *Delle scritture in cifra usate dalla Repubblica Veneta* - Venezia 1873.

(16) A. MEISTER - loc. cit., 1902, pag. 24.

Vari di questi erano del re di Francia con i propri ambasciatori: uno del Vicerè di Napoli; varii pontifici; uno mandatogli dal Re d'Inghilterra, trovato nelle suole di scarpe dorate (sic) provenienti dalla Francia (9 febbraio 1556); altro mandatogli dal Duca d'Alba; ecc.

Al Musefili successe Camillo GIUSTI, indicato come « valente decifratore delle altrui cifre senza controcifra, per l'altezza sua Serenissima » fino al 1586, ed autore di interessanti memorie sui modi di cifrare e sulle cifre straniere (17).

Non si hanno notizie delle cifre napoletane di quell'epoca, ma che esse non fossero da meno delle altre dobbiamo arguirlo dal trattato di G. B. Porta (v. Frontespizi) pubblicato nel 1563 a Napoli, di cui diremo tra poco.

Nel Meister (1902) sono riportate varie cifre dei sec. XV e XVI, usate a Siena, Lucca, Pisa, Genova.

9. Le cifre di Gerolamo Cardano.

9. — Di poco precedente a G. B. Porta è un altro grande italiano, Gerolamo CARDANO (1501-1576), che pur essendosi occupato solo di passaggio di crittografia, in poche dense pagine delle sue due opere più note (18), ci ha lasciato tracce profonde di genialità. Fra le sue cifre quella che più spesso viene citata è la *griglia a finestra*, consistente in un cartoncino avente delle finestre saltuariamente sparse, nelle quali scrivevasi il testo segreto, riempiendo poi gli intervalli in modo da dare al testo un significato diverso ed innocuo; ottenendo quindi una scrittura dissimulata. Ma più interessanti, sebbene passati inosservati, o forse non compresi a causa dello stile molto conciso del Cardano, sono diversi altri artifici, tra i quali riportiamo:

a) l'impiego di vari alfabeti secondo una molto semplice chiave numerica diversa da quelle proposte da Bellaso e da G. B. Porta. Si sostituiscono le lettere del chiaro con il numero d'ordine che esse hanno nell'alfabeto regolare (A=1; B=2; C=3...) e si aggiunge cinque (ad esempio), alle prime lettere delle varie parole; 15 (ad esempio) alle seconde; 21 (ad es.) alle terze; 9 alle quarte; oppure (es. della

(17) A. MEISTER - *loc. cit.*, 1902, pag. 42 e 47.

(18) G. CARDANO - *De subtilitate* (1547), pag. 320 - *De rerum varietate* (1577), pag. 801 e 817.

pag. 817): 17 alle lettere della 1^a parola, 9 alle lettere della 2^a parola; ecc. Quindi ai numeri così ottenuti si sostituiscono, come cifre, le lettere corrispondenti nell'alfabeto regolare.

b) una ingegnosa cifra polifona (19) che merita di essere esposta per la sua originalità, notando che una analoga, ma più semplice, era in uso alla corte papale fin dal 1539, da noi attribuita all'ELIO, di cui già si disse [vedi nota (14)].

Ridotte le lettere a 18 (escluse h, j, k, w, v, x, y, z, con la convenzione di sostituire h con un accento, v con u, ed x, z, con s), esse vengono disposte come nella tabelletta qui sotto, e si conviene:

1°) ogni lettera delle due ultime colonne si cifra con la maiuscola corrispondente sulla sua linea e si mette come iniziale di un gruppo ci-

A	a e	r n	c b
B	i o	d l	g q
C	u s	m f	p t

frante; 2°) ogni lettera della seconda colonna si cifra con la maiuscola corrispondente e si mette, nel gruppo cifrante, al seguito della cifra precedente; 3°) se il chiaro comincia con una lettera della seconda colonna, vi si metterà a sinistra una lettera nulla, ad esempio una minuscola se il crittogramma è di lettere maiuscole.

Esempio:

Chiaro a t t e n d o o r d i n i
cifre corrispondenti b A C C A A B B B A B B A B

crittogramma bA — C — CA — A — BBB — A — BB — AB

(19) Dobbiamo al cortese concorso dell'amico Gen. V. Gamba l'interpretazione di questa cifra.

Per decifrare si scrivono in colonna, e sotto alle successive cifre, le quattro o le due lettere in linea con dette cifre (nella tabelletta), secondo che queste sono iniziali o interne del gruppo, e si sceglierà quindi, in ciascuna colonna, la lettera che dà un senso al discorso.

Esempio :

crittogramma	C A	A	C A C C	A B	C B
decifre	M A	R	M A U U	R I	M I
	F E	N	F E S S	N O	F O
	P	C	P	C	P
	T	B	T	B	T
chiaro	P A	R	T A S U	B I	T O

10. L'opera classica di G. B. Porta.

Giovanni Battista PORTA 1535-1615), pubblicò nel 1563 il suo Trattato (20) che ebbe poi altre sei edizioni, l'ultima del 1602.

Trattasi di un'opera magistrale che sarebbe ancora oggi apprezzata se fosse stata scritta o tradotta in italiano.

Egli raggruppa la materia in 4 libri; il primo dedicato alle cifre antiche, il secondo alle cifre moderne, il terzo alla decrittografia, il quarto ad una raccolta di parole e di sequenze di parole che per la loro speciale conformazione si prestano ad essere individuate nei crittogrammi dei vari tipi studiati. La esposizione vi è chiara, completa e succinta, contenuta in sole 228 pagine.

Del Porta tutti gli autori posteriori citano una tavola cifrante [da alcuni autori tedeschi attribuita poi a Napoleone I (!)], che rappresenta una netta discesa di fronte alle cifre dell'Alberti e del Bellaso. Ma occorre osservare che G. B. Porta consiglia, nella sua descrizione, tavole molto più sicure, dando, *solo come esempio*, la più semplice e quindi la meno sicura.

(20) IOAN BAPTISTA PORTA, *De Furtivis literarum notis - vulgo de ziferis* - Napoli, 1563 (vedi frontespizi).

E' un indizio di ben scarso acume crittografico quello offerto dai vari commentatori posteriori che, sorvolando sui chiari consigli dell'inventore, hanno considerato ed apprezzato solo la proposta peggiore.

Altro appunto che si può fare a G. B. Porta è di essersi indugiato su un cerchio cifrante con segni di fantasia (anziché con lettere comuni) quando tali segni erano ormai da tutti abbandonati, e di avere consigliato, con detto disco, un ciframento con alfabeti consecutivi

D K B	D M C A I F G H K L N P E O R Z B Q S T U V X Y
M L Q	D M C A I F G H K L N P Y E O R Z B Q S T U V X
C N S	D M C A I F G H K L N P X Y E O R Z B Q S T U V
A P T	D M C A I F G H K L N P V X Y E O R Z B Q S T U
I E U	D M C A I F G H K L N P U V X Y E O R Z B Q S T
F O V	D M C A I F G H K L N P T U V X Y E O R Z B Q S
G R X	D M C A I F G H K L N P S T U V X Y E O R Z B Q
H Z Y	D M C A I F G H K L N P Q S T U V X Y E O R Z B

(orbicolare) che egli stesso insegna poi a decrittare con relativa facilità.

Dopo di che è invece da lodare la scelta accurata delle cifre dei vari sistemi, quali: la trasposizione semplice, una ingegnosa trasposizione con chiave, una cifra per digrammi ed una curiosa per tetragrammi; in questa ogni segno comprende una breve asta verticale alla quale sono uniti, uno in alto e uno in basso, uno a destra ed uno a sinistra, quattro segni elementari, rappresentanti 4 lettere del testo

segreto, secondo una semplice lista convenuta (21). Ma la più interessante è la *cifra con verme letterale*, secondo la quale le successive lettere del testo chiaro sono cifrate con successivi alfabeti, ricavati dalla sua tavola già citata ed indicati dalle lettere di una frase convenuta o di una successione di lettere (chiavi) che appunto si chiama *verme letterale*. Le lettere del verme convenuto si scrivono sotto a quelle del testo chiaro e ciascuna di queste si cifra con l'alfabeto (della tavola cifrante) indicato dalla sottostante lettera del verme.

Per dare un'idea concreta di questi semplici procedimenti riportiamo una tavola cifrante compilata al modo di Bellaso ed impiegata col verme letterale di G. B. Porta. Si sarà fissata una *parola* da cui si debbono derivare gli alfabeti cifranti, esempio: « *Democrazia* » ed un verso poetico come verme, ad es.: « Nel mezzo del cammin di nostra vita, ecc. ». Ridotto ad es. l'alfabeto a 24 lettere (escludendo J W) si scriveranno le lettere della parola D, E, M, O, C...) alternativamente su due righe, eliminando le lettere ripetute e completando le 24 lettere come si vede nella 1^a lista della tabella: si otterrà così il 1° alfabeto, in cui D è cifra e decifra di E; M è cifra e decifra di O; ecc. Gli altri alfabeti si ottengono spostando a destra la seconda riga: di un posto nella 2^a lista; di due posti nella terza; e così via. Se si conviene di usare 8 alfabeti, questi saranno individuati da una delle tre lettere del 1° alfabeto, che si dispongono, incolonnate, nella casella di sinistra. Così il 1° sarà individuato dalle lettere D K B, il 2° dalle M L Q, ecc. Ciò preparato e convenuto tra i due corrispondenti, chi cifra scriverà il testo da trasmettere in lettere maiuscole: poi, sotto ogni lettera del chiaro, metterà una lettera del verme convenuto: quindi in una terza riga (crittogramma), scriverà la lettera che, nella lista individuata dalla lettera del verme, fa coppia verticale con quella del chiaro; essa sarà assunta come cifra: es.

chiaro	D A N O T I Z I E A T T E N D I B I L I
verme	N E L M E Z Z O D E L C A M M I N D I N
cifra	X Y V C P V N Y D Y K L A V Y E G B Q R

Infatti nella 3^a lista (N), il D si cifra con X; nella 5^a (E), l'A si cifra Y, ecc. Identica è la operazione per decifrare, come è evidente. Infatti nella 3^a lista (N) la X dà D; ecc.

(21) Vedere in copertina la cifra di « Un Primato Italiano ».

La cifra a verme letterale di G. B. Porta è meno segreta di quella dell'Alberti, è molto simile a quella del Bellaso ed è di uso semplice, comodo, specialmente adatto per le macchine crittografiche. Queste debbono riconoscere in G. B. Porta il pioniere che ne ha formulato il principio basilare: usare alfabeti involutori, disordinati e vermi letterali molto lunghi (principio della macchina « Enigma »).

I suoi successori hanno invece creduto di progredire consigliando alfabeti regolari e vermi corti, da tenere a memoria, ma facili anche ad essere scoperti!

Nel trattato di G. B. Porta si parla della trasposizione letterale, del linguaggio convenzionale, della griglia a finestre (già descritta dal Cardano), quindi del linguaggio dissimulato, seguendo l'Abate Tritemio, di cui parleremo presto, e si chiude con la cifratura multipla e con il modo di nascondere i messaggi.

Della decrittografia, considerata nel 3° libro, il Porta dà molte e dettagliate regole, con esempi, estese a tutte le cifre descritte nel 2° libro e con l'aggiunta, nel libro 4°, di tutte le sequenze di lettere facilmente riconoscibili nei crittogrammi e che dovevano riuscire di grande aiuto ai decrittatori.

11. *L'Abate Tritemio e B. de Vigenère.*

Di fronte ai nostri Alberti, Simonetta, Silvestri, Bellaso, Cardano, Porta, Soro, Musefli, Giusti, Marin, Amadi, ecc., fuori di Italia, nel XVI sec. troviamo pochi ma assai rinomati competitori, che converrà brevemente passare in rassegna.

(Ioannis Trithemij Abb. Spanh.) vissuto dal 1462 al 1516, famoso

Il primo, e più famoso, è senza dubbio il tedesco abate TRITEMIO scrittore di cose sacre, in sospetto di stregoneria, ed al quale si attribuiscono due opere: la « Poligraphia » pubblicata nel 1518 e la « Steganographia » pubblicata nel 1531, ma che si dice compilata nel 1500. Entrambe in grossi prolissi volumi, nei quali i suoi ammiratori vedono principii ed idee, nascoste sotto un linguaggio oscuro e simbolico, che difficilmente si possono sostenere. Due innovazioni vengono a lui attribuite, di cui la prima non viene discussa, ed è un linguaggio dissimulato, ottenuto mediante una raccolta di alcune centinaia di liste alfabetiche disposte in altrettante colonne; in queste le

26 lettere dell'alfabeto sono individuate, ciascuna, da una parola latina. La particolarità sta nella scelta delle parole delle successive liste, le quali sono così composte che prendendo una parola qualunque in ciascuna delle successive liste, la loro successione dà sempre un senso plausibile al contesto; questo può essere così scambiato con una preghiera o con un racconto più o meno fantastico. Il testo segreto da spedire si ottiene sostituendo le lettere successive del testo chiaro ciascuna con la parola che gli corrisponde nelle successive liste, cominciando dalla prima. A questo linguaggio venne dato il nome di *Avemarie* di Tritemio.

Si può osservare che anche con la migliore selezione delle parole, difficilmente il discorso potrà sempre riuscire tanto coerente da escludere il sospetto di linguaggio dissimulato. Esso inoltre dà luogo a testi enormemente lunghi ed implica il possesso di varie centinaia di liste da tenere strettamente segrete; tuttavia Vigenère racconta che esso è servito, almeno una volta, all'Ambasciatore veneto presso il Sultano Selim, che aveva proibito l'uso di cifre agli ambasciatori; il medico dell'Ambasciata, Lorenzo Ventura, riuscì ad eludere la censura turca usando delle *Avemarie* di Tritemio (Vigenère - pag. 183).

Il solo punto che può essere accreditato al Tritemio deriva dal fatto che quella cifra, e le altre analoghe che egli propone nel seguito, sono vere cifre polialfabetiche a verme lungo. Esse tuttavia richiedono il segreto delle liste cifranti, grave inconveniente alla cui eliminazione mira il concetto di *chiave*, (dovuto ai nostri autori), che regola la successione delle liste alfabetiche da usare; la chiave permette infiniti modi diversi di usare gli stessi alfabeti e, se mantenuta segreta, può da sola garantire una sovente sufficiente ermeticità della cifra, anche se non sono segreti gli alfabeti.

La seconda innovazione attribuita a Tritemio è la *tavola quadrata* da lui presentata in due forme diverse: una detta *tavola recta* (*Recta transpositionis tabula*), l'altra detta *tavola aversa* (*Tabula transpositionis aversa*).

Le due tavole sono costituite: la prima con l'alfabeto regolare e la 2^a con lo stesso ma rovesciato; alfabeti che vengono successivamente spostati di un posto a sinistra passando da una riga alla successiva nelle tavole. Così la prima riga della 1^a tavola sarà A B C D E F... X Y Z; la 2^a sarà: B C D E... X Y Z A; la 3^a C D E F G... Y Z A B; ecc.

Nella 2^a tavola la 1^a riga è Z Y X W V... C B A; la 2^a Y X W V... C B A Z; ecc. Ciascuna di queste righe, posta in corrispondenza con l'alfabeto regolare della 1^a riga, costituisce una lista alfabetica cifrante diversa.

Ora la prima di quelle tavole è stata usata dal VIGENÈRE, già citato, per la cosiddetta *cifra quadrata*, adottando il verme letterale del Porta secondo la seguente semplice regola: cercare la lettera da cifrare sulla 1^a riga della tavola; cercare la lettera indicatrice della chiave nella 1^a colonna di sinistra della tavola; prendere come cifra la lettera che sta all'incrocio della colonna individuata dalla lettera chiara, con la riga individuata dalla lettera chiave. La chiave da usare per ogni lettera risulta semplicemente scrivendo, sotto alle successive lettere del chiaro, quelle del verme convenuto, come abbiamo già visto.

Esempio: (22)

chiaro	U R G E	R I S P O S T A	M I O
chiavi (verme)	D E M O	C R A Z I A D E	M O C
cifra	X V S S	T Z S O W S W E	Y W Q

Questa cifra, relativamente scomoda per la ricerca della cifra e della decifra, è molto più debole delle cifre di Bellaso e moltissimo più debole di quelle dell'Alberti, ma venne ritenuta dal suo autore e dai suoi seguaci, per quasi 300 anni, come la cifra per eccellenza e contesa fra i francesi e tedeschi. Questi ultimi ed i loro seguaci, basandosi unicamente sulla esistenza della tavola nel libro del Tritemio, attribuiscono a questi anche il modo di usarla, che è invece, a nostro parere, indubbiamente del Vigenère che chiaramente lo espone nelle pagine 49 e 50 del suo *Traicté*. In ogni caso si tratta di una cifra che non risulta neppure che sia stata molto usata praticamente, e che tecnicamente è molto al disotto di quelle italiane che la precedettero; le ha molto giovato la fama dei presunti due inventori.

Il libro del Vigenère (fig. 6) ci sembra nettamente superiore ai due del Tritemio, sia per copia di metodi e di cifre diverse, sia per

(22) Per seguire la cifratura basta compilare la tabella recta di Tritemio sopradescritta, oppure sostituire la lettera chiara, di posto x nell'alfabeto, con la lettera di posto $x+y-1$, essendo y il posto della lettera chiave. Es. $U(21)+D(4)-1=24=X$.

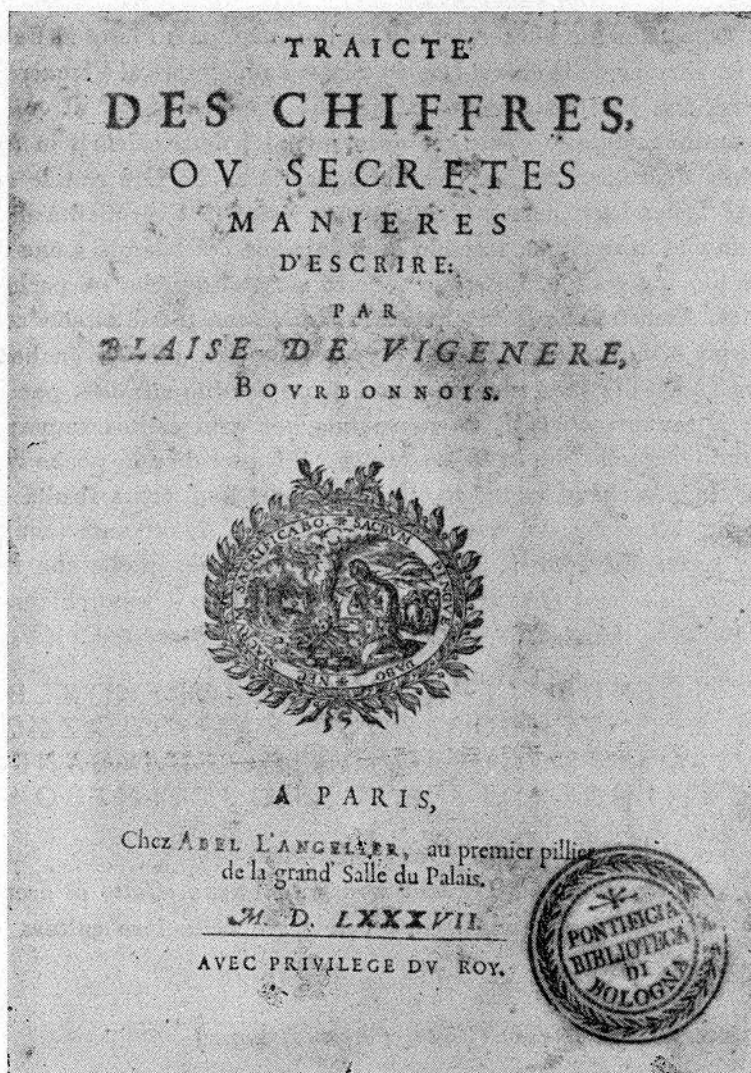


Fig. 6 — Frontespizio del « Traicté des chiffres » di B. de Vigenère

la molto maggiore chiarezza della esposizione, la equanimità dei giudizi in esso espressi, la varietà delle notizie e degli aneddoti di cui è cosperso (fig. 8 e 9).

E' specialmente interessante la attribuzione, da lui fatta al Bellaso, della invenzione delle chiavi (fig. 9). Si deve addebitare al Vigenère una ammirazione sconfinata verso gli antichi magi ed ebrei, di cui egli cita continuamente le opere, le opinioni ed i detti celebri, in interminabili e prolisse pagine che nulla hanno a che fare con le cifre.

Al Tritemio si deve addebitare una oscurità e prolissità di linguaggio che lo rendono, secondo la definizione del Lacroix « una delle opere più indigeste ». Lo stesso tedesco A. Meister che ne parla con rispetto, ammette che le regole del Tritemio sono spesso circondate da esorcismi e da oscurità. Basta osservare che egli diluisce in ben 26 pagine (fig. 7) le successive posizioni di un cerchio cifrante, per ricavarne altrettanti alfabeti, da usare uno per ogni crittogramma; per dire quindi quello che lo stesso prolisso Silvestri dice in poche righe. Senza contare che si tratta di cifre molto ingenue, come risulta dalla qui unita soluzione del crittogramma della fig. 7, ottenuta semplicemente scrivendo, sotto le lettere del crittogramma, quelle che le seguono nell'alfabeto (senza la Y), fino ad ottenere il testo chiaro, lievemente complicato dalla presenza di qualche lettera nulla (M, T.).

cifra	X O F K D B O A F P X O F B C P I F P Q B F K Q X L P B O
	Z P G L E C P B G Q Z P G C D Q K G Q R C G L R Z M Q C P
	A Q H M F D Q C H R A Q H D E R L H R S D A M S A N R D Q
chiaro	B R I N G E R D I S B R I E F S M I S T E I N T B O S E R

(Il latore di questa lettera è un malfattore).

Tanto Vigenère che Tritemio non si occupano affatto di decrittografia, mostrando così una lacuna ben grave nella loro cultura crittografica.

12. I decrittatori celebri (Viète, Partenio, ecc...)

Due parole ancora per i decrittatori. Nelle opere di crittografia che trattano delle cifre del sec. XVI un nome è specialmente noto ed è quello del matematico francese VIÈTE, che al tempo di Enrico IV riuscì a decrittare le cifre usate da Filippo II con i suoi generali

DES CHIFFRES.

36

finiment varier, demeurans renfermees secrettement dans la pensee des consachans; & le chiffre où elles s'appliquent, tout ainsi qu'en vne serrure dont à tous propos on changeroit les gardes, tousiours vn meisme: lequel n'est basti que de nos communs caracteres sil'on ne veult; qui se transportent & changent les vns pour les autres d'infinies sortes par vne reuolution circulaire, ainsi que les *Ziraph* des Hebreux, representez dans le liure de la formation qu'on attribue au patriarche Abraham; mais plus droictement à Rabbi Akiba, ce grãd Talmudiste, qui pour auoir voulu opiniaistrement adherer à deux faulx Messihes nommez *Barcozbas* ou fils de mensonge, fut avec le dernier pris finablement dans Bizerte par l'Empereur Adrian, & martyrisé tres-cruellement; assauoir escorché tout vif par esguillettes, & puis brulé à petit feu, avec quarante autres seditieux, & innumerable nombre de Iuifs mis à mort, quelques six vingts ans apres la natiuité de nostre Sauueur; ausquels encore iusqu'auiourd'huy on celebre es synagogues vn solennel anniuersaire & vn ieusne, le cinquiesme iour de la lune du mois de *Tisri*, qui respond à nostre Septembre.

PREMIEREMENT donques ie mettray le chiffre, que i'attribue quant à moy à vn certain *Belasio* de la suite du Cardinal de Carpi, pour auoir esté le premier de tous ceux dont i'ay eu cognoissance, qui le practiqua & mit en auant l'an 1549. que ie fuz à Rome la premiere fois: Car le liure cy deuant alle-

Fig. 8 — Riproduzione della pagina 36 del «Traicté des chiffres» del Vigenère in cui è citato il Bellaso.

T R A I C T E

gué de Baptiste Porte, auquel il a inferé ce chiffre sans faire mention dont il le tenoit, ne sortit en lumiere que l'an 1563. Et si il le doibt auoir anticipé de quatre ou cinq ans, parce qu'il ne fut en vente que l'an 1568. Aussi le grand Vicaire de saint Pierre cy dessus allegué, qui l'enrichit depuis de tout plein d'vsages, dependans neanmoins du premier fondement, en deferoit l'inuention à iceluy Belasio quant aux clefs; car pour le regard des commutations elles ont esté de tout temps, ainsi qu'il a esté dit cy deuant; & mesmes il y en a force tables en la Polygraphie de Tritheme, mais non gueres bien practiquees. Et pourautant que ces clefs si elles consistent de plusieurs mots tout de suite, comme la plus-part font qui prennent des carmes entiers de Virgile, & autres Poëtes, sont vn peu facheuses, & subiettes à sy traueser, qui est vne mort pour le dechiffreur, i'y ay, de mon inuention puis-ie dire, amené l'artifice de faire dependre toutes les lettres l'vne de l'autre, ainsi que par enchaînement, ou liaison de maçonnerie; & ce par leur collocation & suiuanes, selon que vous pourrez veoir cy apres. Ceste table au reste, soit à Belasio, soit à Baptiste Porte qu'on la vueille attribuer, n'est toutesfois à parler au vray, de l'vn ny de l'autre, ains contretiree sur les *Ziraph* du Iezirah, de 22. lettres pareillement, combien qu'on se puisse passer de vingt, pour en faire vn chiffre carré; & de moins encore, afin de mesnager les autres pour seruir de nulles, & d'vn sens secret reserué à part; ce qui n'a esté

Fig. 9 — Riproduzione della pagina 36 (verso) del « Traicté des chiffres » del Vigenère in cui è citato il Porta e ancora Bellaso.

tori ed autori di trattati di decrittografia, ai quali dobbiamo aggiungere, Pietro PARTENIO, veneto, celebre cifrista del tempo di Viète e che venne incaricato di modernizzare le cifre veneziane quando, per confessione dello stesso Viète (24), questi era riuscito a decrittare in parte anche le più sicure di dette cifre.

Possiamo ora ben concludere che il secolo XVI rappresenta, anche nell'arte delle cifre, un indiscutibile primato italiano sia per la quantità che per la qualità delle opere italiane ad essa dedicate, ma altresì per la arditezza e modernità delle idee in esse espresse, specie dall'Alberti, vero maestro in quell'arte.

La indubbia abilità del Viète ci richiama l'osservazione che le cifre sembrano riuscire particolarmente adatte ai matematici, tali essendo stati essenzialmente Alberti, Porta, Cardano e tale essendo stato un altro celebre decrittatore, J. Wallis, che operava sulle cifre francesi verso la fine del sec. XVII.

Agli ufficiali del Genio, cui non manca una solida base matematica, porgiamo l'augurio che siano preferibilmente affidati i compiti crittografici, e che anche in quelli essi sappiano eccellere come i loro lontani precursori.

(24) E. BAZERIES, *op. cit.*, pag. 234.

TRATTATO DELLA CIFRA

(Roma 1464 - 72)

di LEON BATTISTA ALBERTI

Coloro che sono alla direzione degli affari supremi sanno per esperienza quanto sia importante avere qualche persona fidatissima, a cui poter comunicare decisioni e progetti segreti in modo tale che non se ne debbano mai pentire. E poichè, per la comune perfidia umana, non facilmente lo possono, sono state appositamente inventate quelle maniere di scrivere che si chiamano cifre: artificio certo non inutile, se però non vi fosse chi riesce, con certe accortezze e con intuito, ad interpretarle e spiegarle. E costoro non negò che siano molto utili ai principi, poichè per mezzo loro si possono venire a conoscere le macchinazioni ed i disegni altrui, ma, se non sbaglio, è assai più utile poter far sapere, a chiunque assente si voglia i propri pensieri in modo tale che nessun altro fuor di costui mai sia capace di scoprirli. Da questo nostro opuscolo si ricavano tutti e due i vantaggi. Si apre infatti in esso e si indica la via per svelare ciò che gli altri hanno voluto occultare. E inoltre ti si offre il modo, come vedrai, di occultare assolutamente ciò che tu vuoi tenere nascosto. Mi hanno persuaso di mandare a te questo trattato le presenti condizioni di cose. E, di più, mi ci hanno indotto amici prudenti e a te devotissimi. Se l'opera ti piacerà ne sarò lieto.

Mi trovavo presso Dato nei giardini del Pontefice, al Vaticano, e mentre si parlava, come siamo soliti, di cose relative agli studi letterari, si venne a far le più grandi lodi di un inventore tedesco che riusciva, imprimendo con caratteri, a riprodurre da un dato esemplare, con il lavoro di non più di tre uomini, in cento giorni più di duecento volumi. Con un'unica impressione infatti riproduce una pagina in formato grande. Da qui si passò a lodare la genialità di altri in diverse cose; e Dato sembrò mostrare la più grande ammirazione per coloro che riescono, con i loro accorgimenti d'interpretazione, a rendere chiare ed a spiegare quelle maniere di scrivere, dette cifre, che, dandosi in esse un significato convenzionale a complessi stranissimi di lettere, sono note solo a chi le sappia per accordo preso.

N.B. - I numeri posti a margine indicano le pagine del MEISTER, *Die Geheimchrift im Dienste der Päpstlichen Kurie* - Paderborn, 1906. Le parole tra parentesi sono poste a titolo di spiegazione per completare il periodo.

126

E guardandomi: — Tu, disse Dato, che sempre ti sei occupato di queste arti nascoste e di segreti di natura, che stima hai di questi, chiamiamoli così, congetturatori di cifre e spiegatori di segreti? Hai forse anche tu provato se la tua capacità fosse da tanto? — E io sorridendo: A te che sei il capo della segreteria pontificia, forse capita di doverti servire talvolta di questo modo oscurissimo di scrivere, per affari di stato che intendi debbano rimanere assolutamente segreti. — E' proprio così, rispose Dato, e può anche accadere che desideri, per l'ufficio che ho, di potermela sbrigare da me, senza bisogno di servirmi di un interprete estraneo. Qualche volta infatti ci sono portate lettere, intercettate dagli esploratori, scritte con questi accorgimenti; e possono esser tali da non crederle affatto trascurabili; e se hai su questo punto qualche ritrovato, ti prego di comunicarmelo. — Gli promisi perciò di occuparmene in modo che, per quanto mi bastasse l'ingegno, la sua domanda non rimanesse vana. L'ho fatto dunque; e siccome, per quel che sembra a me, indagando e riflettendo ci sono riuscito in gran parte, ho esposto in questo trattato le mie ricerche sull'argomento, perchè riuscisse più agevole a Dato quanto ho fatto in esecuzione dei suoi desideri, e per offrire, come son solito a fare di tempo in tempo, a chi segue i nostri studi, qualcosa di nuovo, che essi potessero aggiungere alle altre mie trattazioni.

Comincerò dall'espore quale via abbia seguito. Credo che non sarà inutile.

Per poter, dunque, procedere a un'investigazione sistematica, cominciai dal riflettere in che cosa propriamente consista la cifra. E giunsi alla conclusione che potevo definirla: un modo di scrivere con notazioni significanti convenzionalmente ciò che gli scriventi avessero stabilito tra loro, allo scopo che non fossero capiti da altri. Se è così, due cose erano necessarie. Primo: che tra i corrispondenti fosse determinata qualche norma costante e precisa, perchè da quel modo di scrivere l'uno potesse sufficientemente comprendere che cosa l'altro intendesse ordinare, domandare, riferire, ecc. Secondo: che non solo il loro modo di scrivere fosse nuovo e inusitato, ma che rimanesse imperscrutabile alle più accorte investigazioni e ai più acuti congetturatori. Ognuna di queste due cose dipende, se ho veduto bene, dall'uso che le lettere hanno e dal modo come ci serviamo di esse nella scrittura ordinaria. Perciò bisognava considerare prima di tutto come si comportassero le lettere nella scrittura, e di quali elementi consti e si componga la scrittura. Ciò appunto che ho fatto, considerando ripetutamente, con studio e diligenza non piccola, gli elementi della grafia; e vi ho insistito sopra, finchè non son riuscito a scoprire alcuni principii e certe regole molto utili. E quelli che hanno ingegno per queste cose, senza dubbio non negheranno di trovare qui un grande aiuto a raggiungere una completa cognizione delle cifre.

127

Prima, dunque, dirò dei rilievi che ho fatto. Sebbene essi sembrano essere utili soprattutto all'interpretazione delle cifre altrui, però se ne ricavano anche degli avvertimenti perchè tu possa inventare delle cifre più oscure e più intricate a chi tenti interpretarle. Poi aggiungerò varie maniere, alcune già in uso, alcune finora non usate, di comporre cifre; maniere veramente utili e assai adatte, che i più degli intenditori dovranno lodar molto. Per ultimo esporrò una cifra inventata da noi; che, appena l'avrai compresa, l'ammirerai e te ne congratulerai. E comincio.

E' cosa notissima, e subito mi si è presentata alla mente, che i nostri discorsi,

i nostri scritti tutti constano di parole, le parole si dividono in sillabe, le sillabe si compongono di lettere. Ho considerato perciò come si comportino le lettere nella scrittura e quale sia la differenza tra esse. Potrei parlarne a lungo, ma, per restringere quanto più possibile, la differenza delle sillabe risulta dall'ordine e dal numero delle lettere, e così si arriva alle parole intere diverse per suono e per significato. Parliamo prima del numero, e di ciò che è connesso con i rapporti numerici: sotto quest'aspetto, la parte principale l'hanno le vocali. Cominciamo dunque da esse.

Una sillaba, o conterà soltanto di una vocale, o alla vocale sarà unita una consonante, o vi saranno più consonanti unite a una vocale; senza vocale, non si dà sillaba. E per conseguenza, se prendi una o due pagine di un prosatore o di un poeta e disponi separatamente, da una parte le vocali e dall'altra le consonanti, troverai senza dubbio numerosissime le vocali. Dal computo che ho fatto mi sembra di poter stabilire che presso i poeti le consonanti non sono che $\frac{1}{8}$ più delle vocali, e presso i prosatori le vocali sono inferiori, rispetto alle consonanti, approssimativamente nella proporzione detta « sesquitertia » (4:3): vocali 3, consonanti 4.

Se infatti si radunano tutte le vocali di una pagina (di prosatori) e risultano essere, p. e., 300, il numero di tutte le consonanti sarà complessivamente di circa 400. E ho rilevato che tra le semplici vocali — *O* — è la meno frequente; non rispetto alle lettere che indicano consonanti ma rispetto a quelle che indicano vocali. Di rarità quasi eguale è la vocale *A*; anche la lettera *V* (*u*) è, come vocale, piuttosto rara, ma la rende più numerosa la *V* consonante. Di questa, trattando altrove delle lettere e degli altri elementi grammaticali, suggerisco che si scrivesse come una *b* con l'asta incurvata, poichè ha un suono intermedio tra *b* e *u*; tra gli antichi vi fu chi pensò di scriverla come una *f* rivolta: così *f* \mathcal{J} .

Infine ho rilevato che tra le più frequenti tra i latini sono *E* e in primo luogo *I*. Questo è quanto ho osservato sul numero delle vocali.

Passo a parlare dell'ordine delle vocali. Su di esse ho rilevato quanto segue. La vocale *o* è seguita immediatamente da un'altra vocale, senza consonante inter-
posta, oppure è seguita da una consonante che sta tra vocale e vocale.

128

Sulle vocali mi sembra di aver trovato: che dopo la lettera *a* segue non rarissimamente nella stessa parola la lettera *V* (*u* e *v*) e talvolta anche la lettera *O*, ovvero, a causa dei dittonghi (*ae*), segue anche *e*; e infine che nella lingua latina non si è creduto di porre troppo spesso *i* dopo la *a*, sebbene presso i poeti antichi fossero usati *musai*, *animai* e simili (= *musae* etc.). Dopo la vocale *o* forse troverai qualche volta la vocale *i* o anche *v*: ma raramente, e questa più spesso come consonante. Dopo la lettera *o* è frequente *e*. Invece mai ricordo di aver veduto in latino *a* dopo *o*. Dopo la vocale *e* segue la stessa *e* e ugualmente tutte e singole le altre vocali seguono bene dopo la *e*. Lo stesso avviene della vocale *u* e di *i*: anch'esse cioè possono trovarsi raddoppiate (in sillabe diverse): p. e. in « *suus* », e possono seguire ad esse senza eccezione tutte le altre vocali.

Sull'ordine delle vocali sono da fare anche le seguenti considerazioni. Ognuna può trovarsi in principio, in mezzo, in fine di parola: come p. e. in « *aura* ». Ciò che non avviene ugualmente per le consonanti. Infine non si trascuri che a ogni

consonante si può aggiungere qualunque vocale: come anche alle vocali si aggiungono le consonanti, non tutte però ugualmente, come vedrai.

Fin qui delle vocali. Adesso rimane a dire delle consonanti. Parleremo prima del numero, poi dell'ordine.

Mi sembra di aver trovato che nella scrittura la più rara è *g*; *f* e *b* le metto tra quelle abbastanza rare, poi seguono da vicino *c*, *k*, *q*. Invece la massima frequenza ho trovato che l'hanno *s*, *t*, *r*, tanto che quasi superano in numero la vocale *o* e non sono molto superate dalla vocale *a*. Vicine a quelle tre, per frequenza, mi sembra di trovare che seguono *m* e *n*.

Adesso dirò dell'ordine delle consonanti nelle parole. L'ordine delle consonanti vien rilevato o secondo l'aggiunzione o secondo la consecuzione. La differenza è questa: l'aggiunzione si ha quando da una o più consonanti, insieme con una vocale, risulta una sola sillaba: p. e. « stat ». La consecuzione si ha quando la lettera, sia vocale o consonante, è divisa dalla precedente in modo tale che ognuna sia a servizio di una distinta sillaba: es.: ar-ma, cor-pus, e simili. Dunque, prima si parlerà dell'aggiunzione delle consonanti, dopo della consecuzione.

129 In vario modo le consonanti si aggiungono a una vocale per costituire una sillaba. Siccome infatti in qualunque sillaba è necessario vi sia qualche vocale, avviene (25) talvolta che essa sillaba abbia soltanto una vocale p. e. in *arx*, e tal'altra che si aggiunga alla vocale una consonante sola sia che preceda la vocale sia che la segua, talvolta vi sarà una consonante prima e una dopo la vocale. Ancora talvolta vi saranno più consonanti prima della vocale: talvolta più consonanti prima e più consonanti dopo. Per non ritornarci sopra, osservo che in alcune sillabe la vocale è preceduta fin da tre consonanti: p.e. *scri-bo*; ma dopo la vocale non ne seguiranno più di due: p. e. *stans*. E non sarà fuor di luogo anche osservare, che tra due vocali di una parola latina non troverai mai più di quattro consonanti, dovunque si possano pensare interposte. Di queste quattro, subito dopo la vocale non si trova quasi mai altra che *b*, o anche *d*, qualche volta *n*; p. e. *adscriptus*, *subscriptus*, *transtra* (*transtrum* = banco dei rematori).

Ad ogni consonante sola, si aggiunge benissimo qualunque vocale, eccetto che alla lettera *q*, perché ad essa sempre deve seguire la semivocale *u*. E su questo punto mi meraviglia molto l'uso, che ha prevalso nello scrivere, di eliminare la lettera greca *K* della quale abbiamo forse bisogno in parecchie parole, come nel trascrivere le parole greche, p. e. *Kelim* (?), *Kalendas*, e simili. E d'altra parte, quando si è stabilito di aggiungere a *q* la lettera *u*, non si è sufficientemente considerato che a questa lettera *q* la *u* è innata perché essa (*q*) suona *Ku*. (26). Per me io penso che non sarebbe da scrivere *cespitem*, *Ciceronem* con la medesima lettera che *consulem*, *curiam*, *causam* e simili: ma di ciò, parleremo altrove.

Inoltre anche *x* raramente si premette a una vocale eccetto che nelle parole greche; e anche la lettera *Z*, sebbene talvolta la puoi forse trovare, nelle latine, premessa alle vocali in principio; tuttavia questo avviene non frequentissimamente.

(25) Periodo alquanto oscuro; qui si segue il senso della versione Bartoli.

(26) Questa sembra la versione giusta alquanto oscurata da errori di copia nel manoscritto originale.

Finora si è detto in qual modo le singole consonanti precedono, nelle prime sillabe delle parole, le vocali. Ora ricerchiamo come si comporti una consonante singola che segua, sempre nelle prime sillabe, alla vocale.

Mi sembra di aver trovato che dopo le vocali, nelle prime sillabe delle parole possono seguire tutte le consonanti, eccetto poche. Infatti le *j* e *v* consonanti, come anche la *q*, non vengono aggiunte dopo la vocale in nessuna sillaba della parola; la lettera *t* può essere aggiunta, sebbene non con grande frequenza; così la *x*, fuorché dopo la vocale *e*, la troverai raramente, nelle parole latine, seguir la vocale; e ugualmente la lettera *g* rifiuta di essere aggiunta dopo la vocale, almeno che alla *g* non segua *m* o *n*. Tutte invece le altre consonanti come ho detto, si aggiungono dopo la vocale, nelle prime sillabe, liberamente senza che debba seguire un'altra determinata consonante. Ma tra tutte le consonanti, la *c*, la *f*, e la *p* seguono la vocale quasi soltanto se raddoppiate.

130

Fin qui della aggiunzione di una consonante semplice dopo la vocale nelle prime sillabe. Ora si deve parlare di una simile aggiunzione di consonante semplice dopo l'ultima vocale. Son da distinguere due casi: parole monosillabe, parole polisillabe.

Nelle monosillabe troverai seguire alla vocale tutte in genere le consonanti, eccettuate *f*, *g*, *p*, *q*, *j*, e *v*; nelle polisillabe, oltre a queste, non troverai seguire *b*, *c*, *d*, e si potrebbe anche dire, per le parole latine, *l*. Invece tanto nelle polisillabe che nelle monosillabe troverai seguire frequentemente *m*, *n*, *r*, *s*, *t*, *x*. Della lettera *Z* non saprei dire altro se non che è, presso i latini, rarissima in qualunque posizione.

Vengo ora all'aggiunzione di due o tre consonanti, nella quale son da distinguere vari casi. Alcuni gruppi non si trovano mai in fine di parola, o piuttosto dopo nessuna vocale della stessa sillaba, presso i latini; alcuni mai in principio, alcuni si hanno tanto in mezzo, tra vocali, come in principio e in fine di parola. Tra le consonanti che, specialmente agli inizi delle parole, sono preaggiunte in gruppi di due, sempre una sarà *s*, o *l*, o *r*. Ma differiscono tra loro, poichè la *s*, nelle aggiunzioni non la troverai che al primo posto, mentre *r* ed *l* staranno al secondo posto. I gruppi con queste due consonanti, i quali presso i latini non compaiono mai in fine di parola, sono 15, dei quali 7 dove la seconda lettera è *r*, vale a dire *br*, *cr*, *dr*, *fr*, *gr*, *pr*, *tr*; 5 dove la seconda è *l*, vale a dire *bl*, *cl*, *fl*, *gl*, *pl*; e tre che hanno per prima lettera *s*, vale a dire *sc*, *sp*, *st*. Si può anche unirci *sq*. Questi gruppi dunque, mai si trovano in fine di parola.

Quei gruppi invece di due consonanti che si trovano abbastanza in fine di parola e mai in principio sono 5: *nc*, *ns*, *nt*, *nx* (propriamente quindi 4); ad essi aggiungo *ps*, *lx*, *rx*, come p. e. *calx* e *arx*.

La lingua toscana, negli inizi di parola può preporre la *s* a tutte generalmente le consonanti, eccetto che alla *x*. Dei gruppi di due consonanti ve n'è uno che si trova in ogni parte della parola, ed è *st*; p. e. *stat*, *adest*, *restat*. Sui gruppi finali, sarà utile non tralasciare le osservazioni seguenti. L'ultima delle due consonanti aggiunte alla vocale in fine di parola, sarà soltanto *t*, *s*, *x* e inoltre *c*.

A queste quattro non potranno precedere, come penultime, quasi altre che le seguenti: *b*, *l*, *n*, *r*, *p*, *s*; con queste diversità però: che dopo la *b* e la *p* non

131

potrà seguire che la *s*; dopo *l* soltanto *t* o *x*; dopo invece la *n* potranno seguire tutte le quattro lettere dette sopra, cioè *t*, *s*, *x*, *c*.

E dei gruppi di due consonanti basta: si potrebbe forse ancora esaminare quali di essi si trovino più frequentemente nella scrittura, ma da quanto abbiamo detto sopra, questo si vede a sufficienza.

I gruppi di tre consonanti che possono presso i latini essere preaggiunti alla vocale, sono: *scr*, *str*, *spl*. Vi unisco anche *scl*, p. e. *sclavus*; ma la lingua toscana, oltre a questi, ha *sbr*, *sdr*, *sfr*, *sgr*, *spr* dei quali i toscani si servono anche talvolta senza la *r*. In questi gruppi, come vedi, e nei simili (del latino?) la prima delle tre lettere è sempre *s*. Anche dopo la vocale, ma raramente e soltanto in fine di parola, si può fare l'aggiunzione di tre consonanti; p. e.: *stirps*, *urbs*.

Fin qui dell'aggiunzione delle consonanti prima e dopo la vocale. Vengo ora alla consecuzione delle stesse consonanti tra loro, cioè di una all'altra. Si ha la consecuzione, come abbiamo detto, quando nella medesima parola due consonanti saranno poste in modo tale tra due vocali che una sia aggiunta e serva alla vocale precedente, l'altra alla seguente. Per quello dunque che dipende dalle consonanti, è noto che ogni consonante può seguire ad una identica consonante; come avviene quando si raddoppiano, p. e. *bb*, *cc*, *dd*, *ff* e simili. A tale raddoppiamento quasi tutte si prestano; eccetto *x* e inoltre *q*, le quali nelle parole non si raddoppiano. Relativamente alle consonanti, considerate singolarmente, per quel che fa al caso nostro mi sembra di aver trovato ciò che segue. Nella stessa parola, dopo la lettera consonante *b* possono seguire, separatamente, tutte in genere le altre consonanti, ad eccezione di *q*, *x*, *z*. Così anche dopo *l* possono egualmente seguire tutte le consonanti singole, ad eccezione di *j*, *q*, *r*; e dopo la lettera *r* tutte indistintamente, anche *x* sebbene rarissimamente; raramente anche seguirà la *f*, e pur essa rara, la *j* consonante.

132 Dopo la *d* seguirà *j* consonante; seguiranno *b*, *m*, *n*, *s*, *v* consonanti ed *r* e *t*, sebbene per lo più queste lettere assimolino a *sè*, nelle parole, la *d*, che precede, così che risultano raddoppiate. E' da notare però che se queste lettere che ho elencate seguono facilmente (la *d*), non così facilmente invece (la) seguono tutte le rimanenti. Per contro dopo *v* consonante, come dopo *j* consonante, nella stessa parola non seguirà nessun'altra consonante; dopo la *c* nessun'altra che la medesima *c* e *t*; dopo la *f* egualmente nessun'altra che la stessa *f* o anche, nelle parole greche, *t*. Così pure dopo la *p* nessun'altra che *t* ed *s*; dopo la *t*, soltanto *q*; dopo *g* seguiranno isolate e disgiunte (in due sillabe diverse), *m* e *n*; dopo *m* seguiranno, isolatamente, *b* e *p* e forse anche *f*. Seguiranno dunque, o non seguiranno, disgiunte, le consonanti che abbiamo detto e nel modo che abbiamo detto.

E ho osservato, e credo opportuno notarlo qui, che se alla lettera *d*, posta tra vocali, segua un'altra consonante, questa lettera *d* non segue in genere ad altra vocale che alla sola *a*; p. e. *admissus*, *adjuvo*.

Fin qui di due consonanti. Quando poi tra due vocali vi saranno tre consonanti, quasi dovunque troverai che la prima di esse è aggiunta alla vocale precedente, le altre due alla seguente (p. e. *impleo*): Che se alcuno dicesse

che in casi come *transportavi* la *n* e la *s* sembrano aggiunte alla prima vocale, *a*, e in *pistrix* tutte e tre le consonanti essere aggiunte all'ultima vocale *i*, io non lo concederei senza obiezioni. Del resto casi come questi sono rari, e difficilissimo è raccogliarli tutti; noi abbiamo rilevato ciò che avviene più di frequente.

Più interessante è questo, che difficilmente si darà qualche parola latina con tre consonanti tra due vocali, in cui la prima delle consonanti non sia *o*, *b*, *o*, *d*, *o*, *x* o *m*.

Fin qui di tre consonanti. Quasi sempre lo stesso sarà di quattro consonanti poste tra due vocali. Infatti alla prima vocale non se ne aggiungerà più di una e le altre tre si aggiungeranno alla seconda vocale; salvo forse in casi come *transfretari* in cui le due prime consonanti siano aggiunte alla prima vocale. E credo si possa affermare: dovunque tra due vocali si troveranno quattro consonanti, le tre ultime di queste saranno sempre del numero di quelle elencate sopra cioè di quelle che si aggiungeranno a gruppi di tre innanzi alla vocale. E anche mi sembra di aver rilevato, che delle quattro consonanti poste tra due vocali, la prima suole sempre non essere altra che *b*, *c*, *d*, *o* *n*; mentre l'ultima sarà *l* e, frequentemente, *r*.

Abbiamo fin qui detto del numero e della disposizione delle lettere; quali delle vocali si trovino più frequenti negli scritti e quali vocali siano seguite da (date) altre vocali; ugualmente circa le consonanti quali s'incontrino più frequentemente e, quanto al loro ordine, come si comportino le consonanti in agguinzione e in consecuzione.

Da ciò che abbiamo esposto, comprenderai facilmente, se non erro, che è aperto il passaggio e la via, agli ingegni svegli per comprendere e spiegare benissimo ciò che è stato scritto in segni cifrati. Infatti raccolte che si siano di una lettera cifrata, le diversità dei segni, dal loro numero sarà possibile congetturare che ve ne sono tanti di oziosi e, come si dice, di nessuna importanza (nulle), o anche di duplicati, cioè significanti la medesima lettera (omofoni), quanti essi sono in più di venti. Le lettere infatti di cui ci serviamo nello scrivere sono non più di 19; cioè *A B C D E F G I L M N O P Q R S T U X*, aggiungivi se vuoi, *Z*, dunque 20. Tutte le altre saranno superflue (nulle) o duplicate (omofone).

133

Tra tutti questi segni, risulteranno essere vocali quelli che troverai più numerosi e che non staranno troppo distanti tra loro (27); e per le consonanti si avranno, da ciò che abbiamo esposto sopra, indizi per determinare, in base alla loro frequenza e rarità, quali esse siano.

Considerando poi le possibili aggiunzioni e consecuzioni secondo le quali possono raggrupparsi, sempre minore diventa la possibilità che ti rimangano nascoste le astuzie di chi ha scritto in quel modo: ma soprattutto giovano l'esercizio in questa indagine e l'applicarvisi d'impegno.

(27) Questa osservazione è alla base del « metodo della separazione delle vocali » del Valerio, che lo ha esposto nel 1893 (*De la Cryptographie* - 1.^e partie, pag. 17) (L. Sacco, loc. cit., pag. 176).

Non ho detto sopra, e forse è molto utile qui accennarvi, che mi sembra di aver rilevato che in una stessa parola segue spesso, a una vocale, un'altra vocale senza alcuna consonante interposta; che nella maggioranza dei casi tra due vocali non v'è, nella medesima parola, più di una consonante; che abbastanza frequentemente tra due vocali troverai due consonanti, piuttosto raramente tre, assai più raramente quattro.

Fin qui del modo come, per loro stessa natura, si comportano i segni alfabetici nell'uso comune dei latini. Ora dobbiamo dire dei vari accorgimenti nel costruir le cifre. Ma prima è bene spiegare un po' più chiaramente come si riesca, per qualunque cifra in genere, a renderla di più difficile interpretazione. Si deve fare in modo che per quelle vocali e consonanti che più frequentemente ricorrono noi possiamo disporre di più e diversi segni. Così, vi saranno più segni per indicare *e*, ugualmente più per indicare *n*, ugualmente più per indicare *a*, ecc. ecc.; e non ci serviremo sempre del medesimo segno nello scrivere ma ora di uno ora di altri. Gioverà anche la trascuranza dell'ortografia: p. e., scriverò *arogans* con una *r* sola e così ugualmente non raddoppierò mai le lettere. Non aggiungerò a *q* la lettera *u*, mai metterò la *h* e stabilirò per *v* consonante un segno diverso che per la *v* (*u*) vocale. Ed è utile assai, inoltre, e specialmente agli inizi e qua e là nel corpo della lettera, scrivere parole senza vocali o senza consonanti, o gruppi di segni senza alcun senso. Tener presente queste cose, dunque, è utile nello scrivere in cifra.

Torno ora al mio argomento: ripetiamo ciò che si è detto fin dal principio: la cifra è un modo di scrivere con segni significanti convenzionalmente ciò che gli scriventi abbiano stabilito tra loro. Qui dunque è da esaminare in genere quali notazioni si possono usare e che cosa gli scriventi possono aver stabilito tra loro. Tratterò prima, dei segni.

134

I segni letterali possono essere o quelli usati presso di noi latini, A B C D E F G I L M N O P Q R S T U X Z, o altri non in uso presso di noi; tra questi possono usarsi non soltanto quelli di cui si servono, tra i loro connazionali, i Greci, o gli Arabi o altre nazioni nello scrivere i libri; ma soprattutto quelli che ognuno può foggia da sè, come p. e. quelli che constino di punti o di linee o di altri segni stranissimi. E questi avranno questo o quel significato ad arbitrio, non cioè secondo una qualche somiglianza dei segni stessi con le cose dedotte dalla natura, quali si dice che siano le notazioni scritte sugli antichi obelischi degli egiziani; ma bensì avranno il senso che avrà voluto chi le ha inventate. Tuttavia comunque si sia potuto convenire, è evidente che i singoli segni significheranno o una lettera o una sillaba, o una parola o finalmente una intera frase. Quindi: o una normale lettera, p. e. *a* ne significherà una qualche altra p. e. *g*, e così egualmente la *b* ne significherà un'altra p. e. *m*. Con questa convenzione a delle lettere normali si daranno significati anormali, così che esse avranno convenzionalmente valore diverso da quello che hanno nei libri degli antichi; ovvero ci serviremo (di altri segni) al posto di queste lettere semplici. Però potrai non soltanto, come abbiamo detto sopra, servirti di molteplici caratteri, consueti o inconsueti, che, o singolarmente o uniti a due, a tre, a più insieme, abbiano il valore di un'unica lettera; ma viceversa con un solo carattere potrai indicare più lettere, quelle

specialmente che chiamano *combinali* perché spessissimo ricorrono abbinate nella scrittura: tali sono quasi tutte le consonanti che si mettono dopo la lettera *s*, o ugualmente quelle che si pongono innanzi alla lettera *l* o alla lettera *r*. Potrai inoltre stabilire che queste lettere e questi caratteri significhino un'intera sillaba o parola, o anche un'intera frase; p. e. che *a* indichi pontefice; *b* esercito; *d* flotta; *e* denaro; *f* guerra; e in modo analogo *r* significhi che i nemici si sono messi in marcia, *s* che l'esercito ha scarsezza di viveri; e cose simili a piacere. E tutte queste cose potrai stabilire ad arbitrio che vengano significate o con un carattere o con due o con più caratteri consueti o inusitati.

Aggiungi che si può sconvolgere nello scrivere anche l'ordine delle singole lettere, sparpagliandole: p. e. se si stabilisce che la prima lettera, da scriversi e da leggersi, della parola, sia l'ultima della linea (28), che la seconda lettera della medesima parola sia la penultima, e che la quarta (lettera) del messaggio sia la seconda, ecc. e così di seguito per le altre lettere, dopo che si sia stabilito un sicuro ordine nello sparpagliamento. Da ciò comprenderai che v'è anche modo di trasferire le lettere dalla prima alla seconda linea od a qualunque altra linea, tra le molte che vi sono. E questo sistema ha possibilità quasi illimitate, e riesce, per la molteplicità delle combinazioni che possono stabilirsi, parecchio oscuro. Tuttavia poichè l'ordine convenuto rimane costante (29), alla fine un investigatore sagace e acuto riuscirà alla spiegazione, quando vi si metta con impegno.

135

Tutto questo che abbiamo detto della sostituzione delle lettere e del loro sparpagliamento in ordine invertito e spostato, lo potrai ugualmente applicare anche alle sillabe. Inoltre a un'intera parola si potrà dare il significato di un'altra parola qualunque, così che p. e. *ipsum* significhi *hoc*, l'avverbio *pro* significhi *ad*, e *in* significhi *sub*; e simili; ugualmente ai nomi si può dare il valore di altri nomi. Anche per i tempi dei verbi si può convenire che siano indicati i casi dei nomi: p. e. *pater*=lego, *patris*=legebam, *patrem*=legi, *pater*=legam, e così in maniere analoghe, che sarebbe lungo enumerare.

Inoltre si potranno sparpagliare tanto le sillabe quanto, specialmente, le parole quasi in maniere infinite. La più adatta è di prendere un libro, sia poeta, sia prosatore antico, o di comporre una qualche lettera di circostanza in cui si parli di qualunque argomento privato; e in essa siano particelle e parole disperse opportunamente, che servano per quello che vuoi dire. E tali parole, che in tal modo si trovano messe qua e là, e che tu vuoi che siano notate e raccolte dall'amico distante, le indicherai apponendovi dei segni convenuti tra voi. Questi segni consiglio che siano tali da non destare alcun sospetto: p. e., un punto, una virgola, una lineetta nella riga o in margine una cancellatura, una raschiatura e simili. E affinché un dato segno sfugga agli attenti indagatori, potrai aver convenuto che non s'intende con esso indicare precisamente quella data parola a cui è apposto, ma quella immediatamente precedente, o seguente, o opposta

(28) Passo alquanto oscuro. Questo testo sembra il più logico ed aderente al pensiero dell'A.

(29) Osservazione acuta, ancora oggi alla base della soluzione delle cifre di trasposizione.

(quella nella parte simmetricamente opposta della linea?), o distante di un certo numero di parole o di righe da quella segnata.

Ciò che abbiamo detto delle lettere, delle sillabe, delle parole si può ugualmente applicare a intere frasi: dar cioè ad esse altro significato, o spostarle; in modo che esse stiano innanzi agli investigatori come cose scritte su foglie di albero, che siano state disperse dal vento e poi raccolte e disposte disordinatamente.

Vi sono anche altri di simili accorgimenti che forse potrebbero fare al caso, ma quelli che abbiamo finora esposto (credo che) bastino, salvo che tu non aspetti da me quelle insulse cose che alcuni dicono bellissime, come p. e. l'uso di latte, acidi, succo di cipolla, e di altri simili ingredienti: che non si leggono se non scaldati al fuoco, o cosparsi o strofinati con certe polveri, o bagnati con certe acque, o messi al sole: d'altronde (anche essi) hanno la loro utilità.

Anche ciò che dagli antichi si narra della freccia, del cuoio, della lepre, dell'uomo rasato, non sono di tanta importanza, che io debba preferir questi mezzi ad invenzioni le quali, pur essendo migliori (di quelli), non possono nemmeno esse dare sicura fiducia (30).

136

Ma se si trova gusto in simili curiosità, riferirò, a titolo di ricreazione, qualcosa dei nostri segreti. Vi son parti del corpo umano, più nascoste forse, dell'unghia del piede nel giumento, nelle quali potresti scrivere una lettera. non tanto breve, per mezzo di un certo liquido ed in tal modo che si può leggere benissimo anche dopo più di venti giorni, senza che nel frattempo venga cancellato nè dal sudore nè dall'acqua, nemmeno se calda. Trattando tal parti con un'acqua preparata con certi ingredienti, esse si contrarranno e si raggrinziranno in una piccolissima forma sferica, ricoprendosi di una rugosità ruvidissima e spessissima che non lasciano nessun sospetto di scrittura; quando poi saranno trattate con un'altra acqua esse si ridilatano in modo che vi si può leggere con tutta chiarezza. Ma di questi segreti naturali tratterò altrove.

Ora è da dire della maniera di scrivere inventata da noi. Essa ha questi vantaggi: nessuna cifra, tra tutte quelle che si possono usare, è più rapida e più facile a leggersi; nessuna, se tu ignori gli indici convenuti tra me e un altro, si può pensare più segreta. Affermo: che tutti i più acuti e più scaltri ingegni di tutti gli uomini, tutto lo studio dei più intelligenti, ogni capacità, abilità, sforzo, riusciranno vani. Ma nessuno, se non chi è consapevole dell'accordo, potrà riuscire da sè a comprendere qualche cosa di quelle che si trovino scritte con questa cifra nostra. Aggiungi che qualunque comune scrivano può essere da te chiamato a scrivere sotto dettatura in lettere consuete e note, e tuttavia non comprenderà nulla di ciò che avrà scritto. Ugualmente potrà un altro leggere qualunque messaggio mandato a te dalla provincia: tu comprenderai chiarissimamente tutto, e colui al quale l'avrai data perché te la legga, non ne capirà una sola sillaba. A ragione perciò dico che questa è cifra degna dei re, della quale essi possono servirsi, con tutta facilità e con lievissimo lavoro, senza bisogno di interprete che sappia i loro segreti.

(30) Testo oscuro: traduzione a senso.

Ma ora basta di ciò. Andiamo alla cosa. Quella maniera di scrivere occultissima e comodissima, a cui diamo la nostra assoluta preferenza, è la seguente. Faccio due cerchi con due lamine di bronzo: uno maggiore da chiamarsi stabile, l'altro minore che chiameremo mobile. Lo stabile supera il mobile di un nono del diametro di questo. Divido l'intera circonferenza di tutti e due i cerchi in 24 parti di uguale angolo; queste parti si chiamano domicili. Nei singoli domicili del circolo maggiore scrivo le singole lettere maiuscole, in rosso, secondo l'ordine solito delle lettere: per prima A, per seconda B, per terza C, e di seguito tutte le altre; H e K, non essendo il loro uso strettamente necessario, si tralasciano. Saranno dunque queste maiuscole in numero di venti, quali le abbiamo numerate sopra (a pag. 43 - 133 del Meister); e queste lettere, occuperanno altrettanti, cioè venti, domicili delle lettere stabili e vere. I quattro domicili che vi rimarranno vuoti si dicono domicili *numerati*, perchè in ognuno si scriverà il suo numero, a carattere piccolo, in inchiostro nero; nel primo 1, nel secondo 2, nel terzo 3, nel quarto 4. Così tutti i domicili del circolo maggiore saranno occupati da proprie lettere.

137

Nel circolo minore vi saranno altrettanti domicili, uguali di numero a quelli maggiori e in linea corrispondente ad essi. In ciascuno di questi domicili, che si chiameranno mobili, si scriverà una lettera in inchiostro nero, non maiuscola come quelle nel circolo maggiore, ma minuscola. *E non si scriveranno in ordine, ma sparpagiate, così come verranno tra mano a caso* (31); p.e. la prima di queste lettere mobili potrà essere a, la seconda g, la terza c, ecc., finchè non siano occupati tutti i 24 domicili di questo circolo minore. Altrimenti infatti sono, nella scrittura latina, i segni delle lettere; l'ultimo di essi è « & » (et).

Dato in tal modo il proprio segno a tutti questi domicili, adattiamo la lamina mobile, del circolo minore, sopra la maggiore stabile, in modo che il medesimo ago penetri per i centri di ambedue e sia l'asse comune, intorno al quale giri la lamina mobile. Lo strumento così composto di questi due cerchi, lo chiamiamo « *formula* ». Di questa formula bisogna avere due esemplari: una presso di te, una presso l'amico in provincia, al quale tu dovrai scrivere; e tutte due queste formule saranno assolutamente simili, tanto per la collocazione delle lettere come per il loro numero e per il loro ordine, in modo che non differiscano in nulla. Fatto ciò stabiliremo tra noi quale vogliamo che sia l'*indice*; è l'indice infatti quasi una *chiave* con la quale si possa entrare nei sacri penetrali intimi. Tale indice è duplice: uno che è scelto tra le lettere maiuscole stabili, l'altro tra le lettere minuscole mobili; l'uno e l'altro ad arbitrio.

Prima, dell'indice mobile.

Sia p. e. convenuto che l'indice della tabella mobile sia *k*. Io nello scrivere metterò i due cerchi della « formula » come meglio mi piacerà: in modo, p. e., che la lettera convenuta *k* stia sotto la maiuscola *B* e la seguente sotto la seguente. Nello scrivere a te io per prima lettera scriverò *B* maiuscola, sotto la quale ho messo, nell'accingermi a scrivere, l'indice *k*. Questo significherà che anche tu, in provincia, per leggere il nostro messaggio, accomodi, girando la

(31) Norma importante trascurata dai successori dell'Alberti.

« formula » gemella che è presso di te, finché ugualmente l'indice k sia sotto B , con ciò anche tutte le altre lettere (minuscole) trovate nel messaggio verranno a significare il valore e il suono delle lettere stabili superiori.

138 Dopo che avrò scritto tre o quattro parole, muterò nella mia « formula » il posto dell'indice facendo rotare il cerchio, in modo che l'indice k stia p. e. sotto D . Per ciò nel messaggio scriverò allora la maiuscola D ; a cominciar di lì, quindi, k significherà non più B ma D , e le altre singole lettere che seguono acquisteranno diversi significati, dati dalle lettere superiori stabili. E analogamente tu, in provincia, avvertito nel leggere la lettera maiuscola che hai trovato saprai che essa non vorrà dir altro se non indicarti che a quel punto è stata mutata la posizione del cerchio mobile e la collocazione dell'indice. Anche tu perciò metterai l'indice sotto quella lettera maiuscola e in questo modo leggerai e comprenderai tutto con ogni facilità.

Quanto alle quattro lettere mobili che vengano a trovarsi sotto i quattro domicili superiori numerali, quali che esse siano non importeranno, come si dice, alcun significato se prese singolarmente e potranno singolarmente scriversi come prive di valore (nulle). Ma unite insieme o ripetute, daranno per il nostro scopo mirabili vantaggi; dei quali tra poco.

Potremo, altrimenti, fare la scelta dell'indice tra le lettere maiuscole e convenire tra noi, quale di esse (fisse) sia l'indice. Poniamo, per passar subito a un esempio, che tra me e te sia stabilito come indice, B . La prima lettera del messaggio che ti scriverò, sarà una lettera qualunque, scelta a piacere, delle minuscole, p. e. q . Questa lettera tu la porrai, rotando i dischi, nella « formula », sotto la lettera indice B . Con ciò q verrà ad acquistare il suono e il significato di B ; delle altre lettere ci serviremo, nello scrivere, del modo sopra detto per l'indice mobile. Quando poi con questo secondo modo sarà da cambiare la lista della cifra e la posizione della « formula », a quel punto scriverò nel messaggio un'unica lettera e non più (32), delle lettere numerali, cioè di quelle nel cerchio minore che si troveranno sotto i numeri: si prende p. e. quella che significhi 3, o 4, ecc. Questa lettera la collocherò, facendo rotare i dischi, sotto l'indice convenuto B , e proseguirò quindi secondo quel che si debba scrivere, dando alle lettere minuscole il valore delle maiuscole. Anche poi, per sviare sempre meglio gli investigatori, potrai convenire con l'amico a cui dovrai scrivere, che le maiuscole intramezzate (che senza questa convenzione non vi andrebbero affatto) non abbiano alcun valore; e moltissimi altri accorgimenti potrai usare, che sarebbe lungo e inutile esporre.

Perciò, il suono e significato di ogni maiuscola potrà essere indicato, come vedi, in 24 diversi modi; e, viceversa, ognuna delle (ventiquattro) lettere minuscole potrà dare i 20 significati delle maggiori e inoltre quattro numeri; e ciò variando la posizione dell'indice con la rotazione del cerchio (mobile).

(32) Un numero isolato posto nel testo serve così ad indicare il cambio della chiave; questa sarà la lettera che vi corrisponde nel disco interno e che si inserirà nel crittogramma. Un gruppo da 2 a 4 numeri significherà invece una frase, come si dirà in seguito.

Vengo ora all'uso dei numeri, del quale non v'è nulla di più meraviglioso. Le lettere numerali, sono, come ho detto, quelle minuscole che significano i numeri scritti sopra di esse nel disco maggiore. Le numerali danno esse sole il modo per significare, unite a due a tre o a quattro in un esclusivo ordine per volta, 336 intere frasi. Infatti con queste lettere numerali unite a due, p. e. ha (fig. 4) che significheranno, poniamo, 12, e hi che significheranno forse 13, e con simili combinazioni che si possono fare con questi numerali a due a due si indicheranno fino a sedici frasi. Che se poi le medesime numerali si combineranno a tre a tre, p. e. hai che poniamo significhino 123 e aih che significhino 231, avrai modo di indicare fino a sessantaquattro frasi. Se infine si combineranno queste lettere a quattro a quattro, p. e. aihq che significhino 2341, o ihaq che significhino 3124 e così via, si potranno indicare con tali combinazioni fino a 256 frasi. La somma complessiva, quindi, sarà di 336 intere frasi.

139

Il modo di usarne è il seguente.

Comporremo a parte una tavola di 336 linee, nella quale disporremo ordinatamente tutte le singole combinazioni di questi numeri e le metteremo agli inizi delle linee. In questo modo, cioè: al principio della prima linea sarà 11, della seconda 12, della terza 13, della quarta 14, della quinta 21, della sesta 22, della settima 23, e così via di seguito, come abbiamo fatto nella tavola che daremo appresso.

In questa tavola scriveremo accanto ad ogni numero, nelle singole linee, intere frasi convenute a piacere; p. e. dopo il numero 12: « abbiamo fornito di soldati e di frumento le navi che abbiamo promesso ». Simili integre frasi, *ad arbitrio*, scriveremo accanto ad ognuno di tali numeri nella tavola. Di questa mia tavola è necessario che sia un esemplare presso di te. Tu dunque, in provincia, quando ti sarà giunto il mio messaggio e in esso avrai incontrato lettere numerali, noterai i numeri da esse significati, e consulterai la tavola delle frasi intere; in tal modo apprendrai che cosa ti abbia scritto. Di tale accorgimento nello scrivere, niente si può pensare di più breve, di più sicuro, di più adatto e appropriato all'uso per cui servono le cifre. Chi non ammirerà come con due, o tre, o al massimo quattro lettere, che inoltre non sono sempre le stesse ma varie, si possano significare *trecento e trenta e sei* frasi intere e diverse!

E forse è utile avere due tavole numerali presso di me, e che due identiche siano presso di te: in una tavola di ogni coppia siano disposti nell'ordine che abbiano detto i numeri, così che essi si presentino immediatamente, dagli inizi delle linee, a chi legge; nell'altra siano disposte le frasi per ordine alfabetico, sotto le lettere che servono da titoli, affinché chi scrive non le debba cercare a lungo nella tavola ma le trovi rapidamente. Per i titoli delle frasi sarà da regularsi così: quelle che si riferiscono all'*annona*, si porranno sotto il titolo *A*; quelle relative alla condotta delle operazioni belliche, sotto il titolo *B*; quelle relative alle *navi*, sotto il titolo *N*; e analogamente le altre. Tali tavole numerali differiranno tra loro in questo modo: che nelle une, agli inizi delle singole linee vi saranno i numeri e poi seguiranno le frasi; nelle altre i numeri non saranno all'inizio delle linee, ma vi sarà la lettera che fa da titolo, poi seguirà la frase, e alla fine vi saranno i

140

numeri, quali erano stati attribuiti a queste medesime frasi nell'altra tavola correlativa.

Quando dunque debbo scrivere a te una frase, prima la ricerco nella tavola; e, trovatala sotto la lettera che dà il titolo a cui è stata sottoposta, guardo in ultimo i numeri scritti a fianco. Questi numeri io nel debito modo li scrivo nel messaggio, con le lettere che, in quel caso, dalla « formula » della cifra, risultano significare quei numeri. Tu, come ho detto, dal numero ricaverai immediatamente la spiegazione delle frasi.

Quest'opuscolo desidererei che fosse conservato presso i nostri amici, perchè non sia gettato alla profana curiosità del volgo. E' cosa degna di principi, e destinato agli affari supremi. Sii felice.

(segue lista dei 336 gruppi da 11,12..... a 4443, 4444)

141

Questo (che segue) che è comodissimo e bellissimo, e mirabilmente serve per la salvezza dello Stato e per la trattazione degli affari supremi, desidero dedicarlo alla posterità. Con l'uso di queste tavole, con il mezzo fornito da esse, gli assediati e persone lontanissime potranno scambievolmente significarsi che cosa sia da fare: non con l'invio di lettere ma con disposizione o movimento di lumi o di fumo (33), accorgimento che se lo comprendi e rifletti di quanta importanza sia, te ne congratulerai. Di grazia: che cosa di più ammirabile, che aver il modo come, a dispetto dei nemici, annunziare e rispondere, fin dalla più lontana provincia, in un istante, quale sia lo stato delle cose, che cosa desideri che si faccia, che cosa sia da attendersi!

Fine

(33) E' il principio delle segnalazioni semaforiche con gruppi da 2 a 4 segnali.

REGOLE DI DECRITTOGRAFIA

di CICCIO SIMONETTA (34)

Pavia, giorno III della luna di Luglio 1474

1. — Anzitutto bisogna accertare se il testo è steso in latino oppure in volgare, la qual cosa potrai apprendere in questo modo: guarda se le parole da decifrare hanno soltanto cinque diverse finali oppure meno, oppure più: invero se le finali sono soltanto cinque o meno, puoi giudicare che il testo sia di volgare, mentre se sono più di cinque puoi ritenere che il testo sia in latino; ciò perchè tutte le parole del volgare della nostra lingua terminano con una vocale e le vocali sono cinque: A, E, I, O, U. Se invece le parole del testo avranno un numero di finali maggiore di cinque, puoi stimare che il testo sia in latino e ciò perchè le parole latine oppure « litterales » possono terminare con una vocale, oppure con una semi-vocale: l, m, n, r, s, x, o una muta come: b, c, d, f, g, h, q, p, t.

2. — Altra regola allo stesso scopo di conoscere se il testo proposto è in volgare oppure in latino ovvero « *littera* ». Verifica se nel testo da decifrare si moltiplichino ovvero appaiano di frequente parole rappresentate soltanto da una cifra perchè se ciò accade è verosimile che il testo sia in volgare e ciò perchè nel volgare le parole rappresentate da una sola cifra sono molto frequenti mentre sono rare in latino oppure in « *littera* »; in latino le parole rappresentate da un'unica lettera o cifra sono soltanto 4 e cioè le preposizioni e, a, l'avverbio vocativo o e il verbo imperativo i, le quali parole monolettere di rado si trovano nei testi ad eccezione della preposizione a.

3. — Inoltre esamina se nel testo proposto si moltiplicano e sono frequenti parole di due oppure tre lettere o cifre, e deducine allora che il testo è in volgare; ciò perchè parole di tal genere sono più frequenti nel volgare che nel latino.

4. — Quando dunque per mezzo delle regole predette ti sembra che il testo proposto sia in volgare, oppure sia in latino oppure in « *littera* », se sarà in volgare potrai subito accertare quali cifre ti rappresentino le vocali in genere e ciò perchè le cifre che si trovano alla fin delle parole sono sempre vocali negli idiomi di tutta l'Italia.

Dopo che col sistema ora detto ti saranno note le vocali, considera quale, tra le cifre che si trovano alla fine delle parole, si ripete più di frequente nei monosillabi e nelle monolettere oppure monocifre, perchè è possibile ed abbastanza

probabile che tale cifra rappresenti la *e*; ciò perchè questa è un verbo ausiliare molto frequente nelle parole del volgare ed appare spesso anche come congiunzione.

5. — Inoltre nei testi volgari farai molta attenzione alle parole di due cifre soltanto, perchè molte di queste cominciano con *l* e ciò perchè gli articoli che si prepongono ai sostantivi sono *lo* e *la* al singolare, e *li* e *le* al plurale.

6. — Così pure bisogna considerare le parole di tre cifre soltanto e osservare se qualcuna di queste spesso si ripete nel testo proposto; ciò perchè la parola *che* spesso si ripete nel volgare.

7. — Se invece ti sembrerà che il testo sia in latino e non in volgare, considera allora le cifre che sono alla fine delle parole e fra queste osserva quelle che più spesso si ripetono perchè è probabile che esse siano: o vocali, oppure *s*, oppure *m*, oppure *t*; ciò perchè la maggior parte delle parole latine hanno desinenza in vocale od in *s*, o in *m*, o in *t*, e poche di esse terminano in una muta che non sia la *t*, ad eccezione di: *ab*, *ad*, *quod* che sono abbastanza frequenti nei testi.

8. — Altra regola (per il latino). Esamina se nel testo c'è qualche parola rappresentata da un'unica cifra e deducine che quella cifra rappresenta *a* perchè nei testi latini raramente figurano parole di una sola lettera che non sia la preposizione *a*, come sopra si è detto.

9. — Altra regola (per il latino). Esamina le cifre che si trovano alla fine delle parole e che, come già detto, spesso rappresentano qualche vocale, oppure *s*, oppure *m*, oppure *t*, e guarda se qualcuna di queste la ritrovi in parole di una o due cifre; se la ritrovi in una parola di una cifra allora questa cifra rappresenta una vocale perchè nessun monosillabo nè sillaba può resistere senza vocale e questa vocale potrà essere *a* e *i* o *u*, ma è più probabile che sia la preposizione *a* come sopra si è detto. Se invece la ritrovi in una parola di due cifre allora ripassati nella mente tutte le parole di due lettere soltanto e specialmente quelle che più spesso ricorrono nei testi come: *et*, *ut*, *ad*, *si*, *me*, *te*, *se*. Ed affinchè non te ne dimentichi qualcuna, ti scriverò qui di seguito tutte le parole di due lettere soltanto, ovvero la massima parte di esse che sono: *ab*, *ac*, *ad*, *an*, *at*, *da*, *de*, *do*, *ea*, *ei*, *eo*, *et*, *ex*, *es*, *he*, *hi*, *id*, *ii*, *in*, *ir*, *is*, *it*, *me*, *na*, *ne*, *ni*, *ob*, *os*, *re*, *se*, *si*, *tu*, *te*, *ve*, *vu*; *ut*.

10. — Altra regola (per il latino). Esamina se nel testo vi sono parole di tre cifre soltanto, di cui la prima sia la stessa oppure simile all'ultima, perchè probabilmente questa parola rappresenterà *non* che spesso ricorre nei testi, oppure *sis*, ovvero *ibi*; ed esamina anche le altre parole di tre lettere di cui la prima sia simile all'ultima come: *ala*, *ama*, *ana*, *ara*, *ede*, *eme*, *ere*, *ehe*, *ixi*, *ivi*.

11. — Altra regola (per il latino). Esamina se nel testo ci sia qualche parola o parole in cui una cifra appaia triplicata dopo un intervallo perchè tale cifra rappresenterà *u*, ad es.: « *ut uvula* ».

12. — Altra regola (per il latino). Considera se nel testo qualche cifra è doppia, specialmente nelle parole di 4 cifre, perchè probabilmente tale cifra rappresenterà *l* oppure *s* che spesso sono doppie come in *esse* ed *ille*.

13. — Altra regola ed ultima, comune sia ai testi volgari che a quelli latini. Esamina se nel testo c'è qualche cifra a cui sempre ed ovunque faccia seguito una stessa cifra, perchè la prima cifra rappresenterà *q*, e l'altra che la segue rappresenterà *u*; ciò perchè dopo *q* viene sempre *u*; inoltre la cifra che segue quella rappresentante *u* è sempre una vocale, perchè dopo la sillaba *qu* viene sempre un'altra vocale.

Tuttavia le regole predette possono essere rese inutilizzabili in molti modi, sia scrivendo in cifre una parte del testo in volgare ed una parte in latino; oppure interponendo ed aggiungendo al testo delle cifre che non rappresentino alcuna lettera (nulle) e ciò specialmente nelle parole di una o due oppure tre cifre o lettere; od anche cifrando con due alfabeti completamente diversi; od infine cifrando *q* ed *u* con la stessa unica cifra.

I N D I C E

1 - Origine e scopi della crittografia	<i>pag.</i> 7
2 - Nasce in Italia la crittografia moderna	» 9
3 - Il Trattato di Leon Battista Alberti	» 12
4 - Il disco cifrante di Leon Battista Alberti	» 14
5 - Le regole decrittografiche di Cicco Simonetta	» 18
6 - Il contributo di Jacopo Silvestri	» 19
7 - Le chiavi e l'opera di G. B. Bellaso	» 19
8 - I primi Uffici Cifra (Roma, Venezia, Firenze, ecc.)	» 21
9 - Le cifre di Gerolamo Cardano	» 23
10 - L'opera classica di G. B. Porta	» 25
11 - L'Abate Tritemio e B. de Vigenère	» 28
12 - I decrittatori celebri (Viète, Partenio, ecc.)	» 32
<i>App. n. 1</i> - Il Trattato della Cifra di L. B. Alberti	» 37
» » 2 - Le regole decrittografiche di Cicco Simonetta	» 51
